引 言

解代数方程是古典代数学的主要内容. 学过中学代数的读者对一、二次方程的求解方法一定很熟悉，很自然地，会进一步提出这样的问题：三次方程、四次方程以至更高次的代数方程应如何求解呢？ 实际上经过数学家的长期努力，一般三次方程、四次方程的公式求解方法在16世纪已经找到了. 可是高于四次的方程的一般代数求解方法，虽然经过许多著名的数学家二百多年的努力(从16世纪中直到18世纪末)，却始终没有被找到(这里所谓代数求解方法，是指经过有限次加、减、乘、除和开方运算来求得方程根的精确解法，而不是指如秦九韶法、牛顿法等的近似数值解法. 这些数值解法在应用上是很有意义的. 但是与我们所要讨论的求解方法是两类性质不同的问题). 为了求解一般的五次方程，曾经枉然地耗去了许多精力. 可是尽管许多人在这个问题上碰了壁，然而却从未怀疑过这种求解方法是否存在！ 直到1770年，法国的数学家拉格朗日 (J. Lagrange 1736～1813) 才开始认识到求解一般五次方程的代数方法可能是不存在的. 他在一篇长达200多页的文章《关于代数方程解法的思考》中，系统地分析总结了在他以前人们所已知的解二、三、四次方程的一切方法，以及他所创造的求解二、三、四次方程的统一方法. 他指出这些解法对于求解一般五次方程都是无效的，并开始认识到根的排列与置换理论是解代数方程的关键所在. 这就开创了用置换群的理论来研究代数方程的新阶段. 在此基础上，

挪威数学家阿贝尔(N. H. Abel 1802～1829)利用置换群的理论给出了高于四次的一般代数方程的代数求解公式不存在的严格证明. 以后法国数学家伽罗华(E. Galois 1811～1832)更进一步证明了不能用代数方法求解的具体方程式的存在,他还用置换群的理论彻底阐明了代数方程可用代数方法求解是依据了怎样的原理. 这后来发展成当今代数学中有趣而又很基本的一部分——群论中的伽罗华理论.

本书的目的,是在中学代数的基础上,介绍如何用置换群的理论研究代数方程的求解问题. 阐明为什么五次以上的一般代数方程不能用代数方法求解,以及代数方程可以求解的根本原理是什么,并用这一理论证明为什么"有限次使用圆规、直尺三等分任意角"等著名难题是不可能的.

我们希望这本小册子能引起中学数学教师及爱好数学的中学生的兴趣. 读了以后能对群论这一近代数学中引人入胜的重要分支,及其在代数方程求解问题中的应用有一个初步了解;为进一步学习近世代数提供一本入门书.

因为我们的希望是比较通俗地讲清楚伽罗华理论的思路,而并不追求严格的推导和证明,所以有些比较冗长或需准备知识较多的证明我们就略去了,只是通过一些具体例子来说明一下.

由于笔者的数学和文字素养都不高,错误在所难免,谨向提出宝贵批评意见的同志表示感谢.

目　录

引　言

一、代数方程的古典解法 ……1

1. 一次、二次方程的求解 ……1

2. 三次方程的解法 ……4

3. 四次方程的解法 ……11

4. 高于四次方程的求解问题 ……14

二、用根的置换理论解代数方程 ……17

1. 利用根的置换解二次方程 ……18

2. 利用根的置换解三、四次方程 ……20

3. 一般五次(或五次以上)方程的代数求解问题 ……27

三、置换群及其重要性质 ……33

1. 置换的乘积及其基本性质 ……34

2. 置换群的概念 ……37

3. 一般的群的概念 ……39

4. 群的重要性质 ……43

四、数域与代数式的可约性．代数方程的伽罗华群 ……56

1. 数域与代数多项式的可约性 ……56

2. 域的扩张．扩张的维数 ……59

3. 代数方程的根域．正规域 ……63

4. 数域的自同构群 ……66

5. 代数方程的伽罗华群 ……75

6. 求代数方程的伽罗华群的具体方法 ……77

五、代数方程的代数解法．尺规作图问题 ……82

1. 尺规作图问题 ……82

2. 代数方程可用代数方法求解的准则 ……85

3. 三次方程的不可约情况 ……91

一、代数方程的古典解法

1. 一次、二次方程的求解

解代数方程是古典代数学中基本的组成部分．本书讨论的一元n次代数方程(以后简称为方程)，一般地可以写成：

$$a_0x^n+a_1x^{n-1}+\cdots+a_n=0,\quad (a_0\neq 0) \tag{1.1}$$

其中n是正整数，称为此方程的次数，a_0, a_1, $\cdots$, a_n等系数是复数，特别地也可以是实数．n次代数方程必定恰有n个根，这就是著名的代数基本定理，德国大数学家高斯(K. F. Gauss 1777～1855)在1799年给出了第一个证明．但是高斯的证明和以后的一些证明方法都不是构造性的，也就是说仅仅肯定了根的存在性，而并未给出具体求根的方法．因此，在高斯之前和之后，人们对于解方程的方法都作了长期的艰苦探索．

代数方程可以根据它的次数来分类．其中一次方程最简单，它的一般形式是

$$ax+b=0,\quad (a\neq 0) \tag{1.2}$$

它的解是

$$x=-\frac{b}{a}. \tag{1.3}$$

二次方程的一般形式是

$$ax^2+bx+c=0,\quad (a\neq 0) \tag{1.4}$$

它的解法也不难．古代巴比伦人早就会用配方法来求解了．

虽然这些内容已为大家熟知，但为了下面讨论方便起见，我们简要地回顾一下：

将(1.4)化为

$$x^2+\frac{b}{a}x+\frac{c}{a}=0, \tag{1.5}$$

配方 $$\left(x+\frac{b}{2a}\right)^2+\frac{c}{a}-\frac{b^2}{4a^2}=0,$$

移项 $$\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}.$$

两边开方(在复数范围里这总是可行的)再移项，即得熟知的一元二次方程的求解公式：

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}. \tag{1.6}$$

在方程(1.5)中，如令 $p=\frac{b}{a}$, $q=\frac{c}{a}$ 则公式(1.6)也可写成

$$x=-\frac{p}{2}\pm\sqrt{\left(\frac{p}{2}\right)^2-q}. \tag{1.7}$$

总之，一次方程和二次方程的根都可以用它的系数的代数式(就是只含有限次加、减、乘、除和开方五种代数运算的表达式)来表示. 所以我们说一次方程、二次方程可以用代数方法求解.

一次方程(1.2)当 $a\neq0$ 时，它的解总是存在的，而且也是唯一的.

二次方程 (1.4) 的根的情况就比较复杂. 从求解公式(1.6)可以看出此时 b^2-4ac 起着重要作用，我们称它为方程(1.4)的判别式，并记为

$$\Delta=b^2-4ac. \tag{1.8}$$

当 a, b, c 为实数时，由求解公式(1.6)易知：

(1) 当 $\Delta>0$ 时，方程(1.4)有两个不相等的实根；

(2) 当 $\Delta=0$ 时，方程(1.4)有两个相等的实根，这个根又称为二重根：$x=-\frac{b}{2a}$，所以此时不需开方即可求得其解；

(3) 当 $\Delta<0$ 时，方程(1.4)有一对共轭的虚数根.

若将二次方程(1.4)的两个根记为 x_1、x_2，则通过直接计算，容易证明它们和方程的系数之间有下面的关系式：

$$\begin{cases} x_1+x_2=-\frac{b}{a}, \\ x_1x_2=\frac{c}{a}. \end{cases} \tag{1.9}$$

这就是有名的韦达(F. Viete. 1540～1603)公式，有的书上也称为韦达定理. 我们特别指出：

$$\Delta=a^2(x_1-x_2)^2. \tag{1.10}$$

它的证明是很容易的，如下：

$$(x_1-x_2)^2=x_1^2-2x_1x_2+x_2^2=(x_1+x_2)^2-4x_1x_2$$
$$=\frac{b^2}{a^2}-\frac{4c}{a}=\frac{b^2-4ac}{a^2}.$$

我们来看一个特殊的二次方程

$$x^2+x+1=0. \tag{1.11}$$

根据求解公式(1.6)易知它的两个根是 $\frac{-1+\sqrt{3}i}{2}$ 和 $\frac{-1-\sqrt{3}i}{2}$. 令

$$\frac{-1+\sqrt{3}i}{2}=\omega. \tag{1.12}$$

则由直接计算易得

$$\omega^2=\left(\frac{-1+\sqrt{3}i}{2}\right)^2=\frac{-1-\sqrt{3}i}{2},$$

因此 ω, ω^2 是方程(1.11)的两个根．而且它们还满足下列关系式：

$$\begin{cases} \omega^2+\omega+1=0, \\ \omega^3=1. \end{cases} \tag{1.13}$$

这是两个下面有用的关系式．其中第一个只要用 ω 代入(1.11)即可，而第二个则是因为

$$\omega^3-1=(\omega-1)(\omega^2+\omega+1)=0.$$

由此还可得：任何一个复数 a 如果 $\sqrt[3]{a}$ 是 a 的一个三次方根，则 $\sqrt[3]{a}\,\omega$, $\sqrt[3]{a}\,\omega^2$ 就是另两个三次根．

2. 三次方程的解法

上面已经看到一次方程、二次方程的求解早已有了很完美的代数方法，我们可以很方便地根据求根公式求出它们的全部根．人们自然会想到，三次、四次以至更高次的代数方程是否也有类似的求根公式？或者说，能不能把一个方程的根用该方程的系数的代数式表示出来呢？再强调一下，这里的代数式是指有限次地使用加、减、乘、除、开方运算得到的．

关于这方面的问题，16 世纪的意大利数学家们首先作出了很大的贡献．意大利当时有一所欧洲最大也是最著名的大学——波罗尼亚大学．波罗尼亚大学的菲尔洛 (S. D. Ferro 约 1465～1562) 教授在 1514～1515 年期间把三次方程全都简化为三种简单的类型：

$$x^3+px=q,\ x^3=px+q,\ x^3+q=px,$$

其中 p, q 均为正数．并对它们进行了系统的研究，不过他从未发表过他的解法，仅把他的研究结果告诉了他的几个朋友．他去世后不久，意大利威尼斯的数学家塔尔塔利亚 (N.

Tartaglia 约 1499～1557) 在 1535 年又重新发现了菲尔洛教授的方法．而且在公众的场合中进行过三次方程求根表演．不过，他仍旧将方法保密．最后，他将这方法透露给意大利米兰的数学家卡当 (H. Cardano 1501～1576)． 卡当背弃了他要为此保密并不能公布该方法的诺言，在 1545 年发表一本著名的代数著作«大法»，在这本著作里他总结了前人的结果，将一般形式的三次方程的求解公式公布了．这个方法后来常称为卡当方法，相应的求根公式通称为卡当公式．

卡当方法简介如下：

一般的三次方程

$$ax^3+bx^2+cx+d=0,\quad (a\neq 0) \tag{1.14}$$

可化为

$$x^3+\frac{b}{a}x^2+\frac{c}{a}x+\frac{d}{a}=0. \tag{1.15}$$

在作了一个简单的代换 $y=x+\frac{b}{3a}$ 后，即可将(1.15)化为：

$$y^3+\frac{3ac-b^2}{3a^2}y+\frac{2b^3-9abc+27a^2d}{27a^3}=0. \tag{1.16}$$

由此可见，求解一般三次方程(1.14)的问题可以归结为方程

$$x^3+px+q=0 \tag{1.17}$$

的求解问题．下面就来讨论(1.17)的求解问题．

再作代换

$$x=z-\frac{p}{3z}, \tag{1.18}$$

则(1.17)化为

$$z^3-\frac{p^3}{27z^3}+q=0,$$

即

$$z^6+qz^3-\frac{p^3}{27}=0. \tag{1.19}$$

将(1.19)看作z^3的二次方程，即可解得

$$z^3=-\frac{1}{2}q\pm\sqrt{\frac{1}{4}q^2-\frac{1}{27}p^3}. \tag{1.20}$$

在上式中取正号并把这时的z改写成u，则

$$u^3=-\frac{1}{2}q+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3},$$

取上式右边的任何一个立方根为u，则三个立方根为

$$u,\ u\omega,\ u\omega^2.$$

为了利用$x=u-\frac{p}{3u}$求x，要先求$-\frac{p}{3u}$. 由于

$$\left(-\frac{p}{3u}\right)^3=-\frac{p^3}{27}\frac{1}{u^3}=\frac{-\frac{p^3}{27}}{-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}$$

$$=\frac{\left(-\frac{q}{2}\right)^2-\left(\frac{1}{4}q^2+\frac{1}{27}p^3\right)}{-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}$$

$$=-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}.$$

所以$-\frac{p}{3u}$是$-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}$的一个立方根，而且应取与$u$相乘为$-\frac{p}{3}$的那个立方根，把它记为$v$. 由$\omega^3=1$，得

$$\begin{cases} x_1=u-\dfrac{p}{3u}=u+v,\\ x_2=u\omega-\dfrac{p}{3u\omega}=u\omega+v\omega^2,\\ x_3=u\omega^2-\dfrac{p}{3u\omega^2}=u\omega^2+v\omega. \end{cases} \tag{1.21}$$

其中u, v分别是$-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}$、$-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}$的一个立方根，且要取得使$uv=-\frac{p}{3}$. 如果写得更仔细些，就是

$$\begin{cases} x_1=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}, \\ x_2=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}\,\omega+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}\,\omega^2, \\ x_3=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}\,\omega^2+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}\,\omega. \end{cases}$$

由于复数开方时$\sqrt[3]{\ }$代表的值不定，这里规定其中

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}} \quad 和 \quad \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}}$$

要取得两者乘积为$-\frac{p}{3}$.

现在我们假定(1.17)的系数是实数，并讨论(1.17)的根的情况. 要研究实系数三次方程的根的性质，和二次方程相似，我们需要引进判别式：

$$\Delta=\frac{1}{4}q^2+\frac{1}{27}p^3. \tag{1.22}$$

$\left(可以证明\ \Delta=-\frac{1}{108}(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2\right)$

(1) $\Delta>0$; 此时

$$-\frac{1}{2}q+\sqrt{\frac{q^2}{4}+\frac{1}{27}p^3} \quad 和 \quad -\frac{1}{2}q-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$$

都是实数且不相等. 令u与v分别是它们的一个实的立方根，则由(1.21)即得

$$x_1=u+v,$$

$$x_2=u\omega+v\omega^2=-\frac{1}{2}(u+v)+i\frac{\sqrt{3}}{2}(u-v),$$

$$x_3=u\omega^2+v\omega=-\frac{1}{2}(u+v)-i\frac{\sqrt{3}}{2}(u-v).$$

所以在 $\Delta>0$ 时，方程(1.17)有一个实根和两个互为共轭的复数根；

(2) $\Delta=0$；此时有 $u=v$，令 u 为 $-\frac{q}{2}$ 的实数立方根，且因 $\omega+\omega^2=-1$(见(1.13))，由(1.21)即得

$$x_1=2u,\ x_2=-u,\ x_3=-u.$$

所以在 $\Delta=0$ 时，方程(1.17)的三个根都是实根，且有两个相等；

(3) $\Delta<0$；这时卡当公式的立方根内已经不是实数而是虚数了，于是它们的立方根也都是虚数．这时我们可以证明 u、v 是共轭复数．这是因为这时

$$u=\sqrt[3]{-\frac{q}{2}-i\sqrt{-\frac{1}{4}q^2-\frac{1}{27}p^3}},$$

$$u\bar{u}=|u|^2=\sqrt[3]{\left|-\frac{q}{2}+i\sqrt{-\frac{q^2}{4}-\frac{p^3}{27}}\right|^2}$$

$$=\sqrt[3]{\frac{q^2}{4}-\frac{q^2}{4}-\frac{p^3}{27}}=-\frac{p}{3}=uv.$$

(这里因为 $|u|^2$ 是实数，$\sqrt[3]{}$ 取实根)所以 $\bar{u}=v$.

既然 u、v 共轭，故可令 $u=a+bi$，$v=a-bi$，于是由(1.21)得

$$\begin{cases} x_1=u+v=2a, \\ x_2=-\frac{1}{2}(u+v)+i\frac{\sqrt{3}}{2}(u-v)=-a-b\sqrt{3}, \\ x_3=-\frac{1}{2}(u+v)-i\frac{\sqrt{3}}{2}(u-v)=-a+b\sqrt{3}. \end{cases}$$

因此在这种情况，所得的三个根都是实根，而且互不相同.

我们注意到对于 $\Delta<0$ 的情况，在卡当公式中有一部分即 $\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}$ 出现了虚数，但最后得到的三个根又都是实数，这对于还没有虚数概念的 16 世纪数学家是难以接受的. 他们认为实系数的方程在最后得到实根的情况下，竟然要借助于包含负数开平方的求解公式来求得其根，这实在太令人费解. 卡当和他同时代的数学家认为 $\Delta<0$ 时既然最后得出实根，求解过程中的虚数一定可以避免，因而费了许多精力想除去卡当公式中的虚数性，但是都没有成功. 只有通过伽罗华的理论才最终把这个问题搞清楚了. 原来在这种情况下，不存在仅包含系数的实数根式的代数求解公式. 通常称 $\Delta<0$ 的情况为不可约的情况. 所以历史上第一次被迫引进虚数的概念，是在研究三次方程不可约的情况的时候，而不是象通常那样认为是对 -1 开平方，或者说是在解二次方程 $x^2=-1$ 的时候，这是一件很有趣的事实. 下面举几个解三次方程的例子.

[例] 解三次方程

(1) $x^3+3x^2+6x+3=0$,

(2) $x^3-\frac{3\sqrt[3]{4}}{2}x+\sqrt{2}=0$.

解 (1) 令 $y=x+\frac{b}{3a}=x+1$，代入原方程化简得

$$y^3+3y-1=0.$$

这里 $p=3$, $q=-1$, $\Delta=\frac{q^2}{4}+\frac{p^3}{27}=\frac{1}{4}+1=\frac{5}{4}>0$.

于是 $$u=\sqrt[3]{\frac{1}{2}+\sqrt{\frac{5}{4}}}=\sqrt[3]{\frac{1+\sqrt{5}}{2}},$$

$$v=\sqrt[3]{\frac{1}{2}-\sqrt{\frac{5}{4}}}=\sqrt[3]{\frac{1-\sqrt{5}}{2}}.$$

故原方程的解为:

$$x_1=u+v-1=\sqrt[3]{\frac{1+\sqrt{5}}{2}}+\sqrt[3]{\frac{1-\sqrt{5}}{2}}-1,$$

$$x_2=\omega u+\omega^2 v-1=-\frac{1}{2}\left(\sqrt[3]{\frac{1+\sqrt{5}}{2}}+\sqrt[3]{\frac{1-\sqrt{5}}{2}}+2\right)$$

$$+\frac{\sqrt{3}}{2}\left(\sqrt[3]{\frac{1+\sqrt{5}}{2}}-\sqrt[3]{\frac{1-\sqrt{5}}{2}}\right)i,$$

$$x_3=\omega^2 u+\omega v-1=-\frac{1}{2}\left(\sqrt[3]{\frac{1+\sqrt{5}}{2}}+\sqrt[3]{\frac{1-\sqrt{5}}{2}}+2\right)$$

$$-\frac{\sqrt{3}}{2}\left(\sqrt[3]{\frac{1+\sqrt{5}}{2}}-\sqrt[3]{\frac{1-\sqrt{5}}{2}}\right)i.$$

这里 $\sqrt[3]{\quad}$ 取实根.

(2) 因

$$\Delta=\frac{q^2}{4}+\frac{p^3}{27}=\frac{(\sqrt{2})^2}{4}+\frac{1}{27}\left(-\frac{3\sqrt[3]{4}}{2}\right)^3=0,$$

所以 $$u=\sqrt[3]{-\frac{q}{2}}=\sqrt[3]{-\frac{\sqrt{2}}{2}}=-\frac{1}{\sqrt[6]{2}}=-\frac{\sqrt[6]{32}}{2},$$

原方程的三个实根为:

$$x_1=-\sqrt[6]{32},\quad x_2=\frac{\sqrt[6]{32}}{2},\quad x_3=\frac{\sqrt[6]{32}}{2}.$$

三次方程 $ax^3+bx^2+cx+d=0$ 的系数和它的根 x_1, x_2, x_3 之间也有与二次方程相类似的关系式. 事实上, 比较方程

$$x^3+\frac{b}{a}x^2+\frac{c}{a}x+\frac{d}{a}=0$$

与 $$(x-x_1)(x-x_2)(x-x_3)=0$$

的系数, 易得:

$$\begin{cases} x_1+x_2+x_3=-\dfrac{b}{a}, \\ x_1x_2+x_2x_3+x_3x_1=\dfrac{c}{a}, \\ x_1x_2x_3=-\dfrac{d}{a}. \end{cases} \tag{1.23}$$

这就是三次方程的韦达公式.

3. 四次方程的解法

四次方程的求根公式和三次方程的求根公式几乎是同时发现的. 卡当的《大法》一书中就已经讲到四次方程的解法. 这个方法是由卡当的学生费拉利 (L. Ferrari 1522～1565) 提出的. 费拉利设法把四次方程化成平方差的形式, 从而把原方程变形为两个二次方程, 然后求得其解. 这个方法通称为费拉利法. 我们简介如下:

任何一个四次方程可以写成:

$$x^4+ax^3+bx^2+cx+d=0, \tag{1.24}$$

将上式用配方法改写成下面的形式

$$\left(x^2+\frac{ax}{2}\right)^2=\left(\frac{a^2}{4}-b\right)x^2-cx-d, \tag{1.25}$$

再以 $\left(\frac{x^2}{2}+\frac{ax}{2}\right)t+\frac{t^2}{4}$ 加于方程(1.25)的两边, 我们就可把它写成:

$$\left(x^2+\frac{ax}{2}+\frac{t}{2}\right)^2=\left(\frac{a^2}{4}-b+t\right)x^2+\left(\frac{at}{2}-c\right)x+\left(\frac{t^2}{4}-d\right), \tag{1.26}$$

为了使右边成为完全平方, 只要选取适当的 t, 使(1.26)的右边的判别式等于零即可, 即

$$\left(\frac{at}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+t\right)\left(\frac{t^2}{4}-d\right)=0,$$

或

$$t^3-bt^2+(ac-4d)t-a^2d+4bd-c^2=0. \qquad (1.27)$$

这是一个关于 t 的三次方程，可利用已知的卡当公式求解. 设 t_0 是它的任何一根，以 t_0 代入(1.26)，(1.26)的右边就配成完全平方了. 即得

$$\left(x^2+\frac{ax}{2}+\frac{t_0}{2}\right)^2=\left(\sqrt{\frac{a^2}{4}-b+t_0}\,x+\sqrt{\frac{t_0^2}{4}-d}\right)^2. \qquad (1.28)$$

这个方程可以分解为两个二次方程:

$$\begin{cases} x^2+\left(\dfrac{a}{2}+\sqrt{\dfrac{a^2}{4}-b+t_0}\right)x+\left(\dfrac{t_0}{2}+\sqrt{\dfrac{t_0^2}{4}-d}\right)=0, \\ x^2+\left(\dfrac{a}{2}-\sqrt{\dfrac{a^2}{4}-b+t_0}\right)x+\left(\dfrac{t_0}{2}-\sqrt{\dfrac{t_0^2}{4}-d}\right)=0. \end{cases} \qquad (1.29)$$

解方程(1.29)，就得到方程(1.24)的四个根. 所以要解一个四次方程，可先解一个三次方程，然后再解两个二次方程就行了.

这里我们可以看到，由于 t_0 是方程(1.27)的根，它可以由方程(1.27)的系数，也即可以由方程(1.24)的系数 a, b, c, d 的代数式表示出来. 而方程(1.24)的根可以由方程(1.29)的系数的代数式表出. 但方程 (1.29) 的系数是由 a, b, c, d 及 t_0 的代数式组成，所以归根到底四次方程(1.24)的根可以由其系数 a, b, c, d 的代数式表出. 这样，我们也证明了一般的四次方程可以用代数方法求解. 但这些表示根的公式比较复杂，在具体计算时用处不太大.

[例] 解四次方程 $x^4+3x^3-3x^2-6x+4=0$.

解 原方程就是

$$\left(x^2+\frac{3}{2}x\right)^2=\frac{21}{4}x^2+6x-4.$$

配方得

$$\left(x^2+\frac{3}{2}x+\frac{t}{2}\right)^2=\left(\frac{21}{4}+t\right)x^2+\left(\frac{3t}{2}+6\right)x+\frac{t^2}{4}-4, \tag{1.30}$$

令
$$\left(\frac{3t}{2}+6\right)^2-4\left(\frac{21}{4}+t\right)\left(\frac{t^2}{4}-4\right)=0,$$

得
$$t^3+3t^2-34t-120=0,$$

解此方程得到一个根 $t=6$, 代入(1.30)式得

$$\left(x^2+\frac{3}{2}x+3\right)^2=\left(\frac{3\sqrt{5}}{4}x+\sqrt{5}\right)^2.$$

开方得
$$x^2+\frac{3}{2}(\sqrt{5}+1)x+(3+\sqrt{5})=0,$$

$$x^2-\frac{3}{2}(\sqrt{5}-1)x+(3-\sqrt{5})=0,$$

解得
$$x_1=\frac{-1-\sqrt{5}}{2},\ x_2=-\sqrt{5}-1,$$

$$x_3=\sqrt{5}-1,\qquad x_4=\frac{-1+\sqrt{5}}{2},$$

这就是原方程的四个根.

一般的四次方程 $x^4+ax^3+bx^2+cx+d=0$ 的系数 a, b, c, d 与它的 4 个根 x_1, x_2, x_3, x_4 之间也存在着类似于二、三次方程的韦达公式:

$$\begin{cases}x_1+x_2+x_3+x_4=-a,\\ x_1x_2+x_2x_3+x_3x_4+x_4x_1=b,\\ x_1x_2x_3+x_2x_3x_4+x_3x_4x_1+x_4x_1x_2=-c,\\ x_1x_2x_3x_4=d.\end{cases} \tag{1.31}$$

4. 高于四次方程的求解问题

如上所述，用代数方法求解三、四次方程的问题在 16 世纪中叶都已得到解决，除了上面介绍的卡当法和费拉利法外，后来还找到了一些其它的求解方法．此后人们的兴趣就很自然地转向寻找一般形式的五次方程或高于五次方程的代数求解公式．

人们企图也能象二、三、四次方程那样找到一个公式，能把五次方程的根用该方程的系数的代数式表示出来．可是前面说过，这一愿望虽然经过许多著名数学家的努力，经历了二百多年的时间，花费了不知多少时间和精力，却始终没有能实现．十七、十八世纪的许多著名数学家，包括欧拉(L. Euler 1707～1783)，都对求解五次方程作过不少努力，也毫无例外地失败了，而且他们总认为这样的公式是存在的，只是没有能找到它而已．

然而他们的努力并非白费，失败者的经验和教训为成功者铺平了前进的道路．到了十八世纪下半叶，法国数学家拉格朗日总结分析了前人失败的经验，开始意识到这种用代数方法求解五次方程的公式可能是不存在的．他在 1770 年发表了《关于代数方程解法的思考》一文，弄清了前人解二、三、四次方程的各种方法看来似乎五花八门，但实质都是基于同一原理．并论述了用于解二、三、四次方程的一些方法为什么不能成功地用于解高于四次的方程．他第一次正确地指出根的排列与置换的理论是解代数方程的关键所在．在本书的第二章里就要介绍这些内容．

拉格朗日虽然没有能彻底解决高次方程的求解问题，但

是他对这个问题所作的贡献是很大的. 正是由于他的工作影响才使阿贝尔和伽罗华等人对高次方程的求解问题的研究走上了正确的道路, 开创了用置换群的理论来研究代数方程求解的新时代.

阿贝尔(N. Abel 1802～1829)是挪威一个乡村牧师的儿子, 幼年丧父, 家境贫困. 他从小学习就很努力, 从中学时起便对数学感到兴趣, 在大学读书的时候, 当时公认的难题——寻求五次方程的代数解法问题同样吸引了他. 有一个时期他曾认为自己已找到了求解五次方程的公式, 但是很快他就发现了自己的错误. 1824 年, 当时只有 22 岁的大学生阿贝尔第一次作出了《五次方程代数解法不可能存在》的正确证明. 这篇具有划时代意义的论文, 以后被收进阿贝尔的全集流传下来, 但在当时却没有被人理解. 据说这篇论文曾送给当时德国的大数学家高斯审阅, 可是高斯也没能认识到这项工作的重要意义. 1825 年以后的四年中, 阿贝尔在数学研究的许多方面都做出了很有创见的成就, 可是阿贝尔的才能与工作在当时欧洲大陆始终没有获得应有的重视. 由于贫病交迫, 1829年 4 月 6 日年轻的阿贝尔死于结核病, 终年仅二十七岁. 这时, 柏林大学已想聘请他为数学教授, 但聘书寄到之日已经是他死后的第三天了.

阿贝尔证明了对所有五次方程都适合的代数求解公式是不存在的, 但是这并不等于说任意一个具体数字系数的五次方程都不能用代数方法求解. 例如, 五次方程 $x^5-1=0$ 确实是可以用代数方法求解的. 这是并不矛盾的, 就象对一元二次方程我们可以断言, 不包含开方的一般求根公式是不存在的. 但是对一个具体数字系数的两次方程, 只要它满足 $b^2-4ac=0$, 就可以不必开方而求得其根 $x=-\frac{b}{2a}$. 例如二次方程

$x^2-x+\frac{1}{4}=0$ 的根 $x=-\frac{-1}{2\times1}=\frac{1}{2}$，不必经过开方运算就可求得．因此，阿贝尔的理论还未解决一个具体数字系数的高于四次的方程是否可以用代数方法求解的问题．这个问题为法国青年数学家伽罗华所彻底解决．他举出了不能用代数方法来求解的具体数字系数的方程，同时他还阐明了方程式可用代数方法求解的条件是什么．

伽罗华 (E. Galois 1811～1832) 是法国巴黎附近一个小村镇镇长的儿子． 15 岁时，由于学习刻苦，他被编在中学的一个数学的特别班里． 当时，他看到了五次方程代数解法所存在的问题，便抓住不放，企图攻克这个难关．但是和阿贝尔一样，最初的尝试失败了．失败并没有使伽罗华灰心丧气，他把当时一些著名数学家欧拉、拉格朗日、高斯等人的著作都找来研究阅读，批判地继承了前人工作的成果，努力探索解决问题的途径．1828 年伽罗华十七岁的时候，把自己写的论文《关于五次方程的代数解法问题》提交给法兰西科学院，可是当时法兰西科学院的一些著名数学家们对他的论文不仅没有认真审阅，反而把它一再丢失．最后，在 1831 年伽罗华第三次写好了论文送交审查，而当时的法兰西科学院的院士泊松写的审查意见是"完全不能理解"．他渴望着进入巴黎著名的工科大学(L'Ecole Polytechnique)，可是接连二次应试都失败了． 最后只能考入高等师范学校（当时叫 L'Ecole Préparatorie，还仅是一个不太好的学校）．这时法国激烈的政治斗争吸引了年轻热情的伽罗华，他两次被捕入狱，并且被学校开除了．1832 年 4 月伽罗华出狱后不久与人决斗受重伤于 5 月 31 日去世，当时还不满二十一岁． 在决斗前夕，他把他关于五次方程代数求解问题的想法与研究结果写成了一封长信，

可是却没有一家出版商愿意刊行这位当时还是默默无闻的青年数学家的遗作。直到14年后，1846年，法国数学家柳维尔(J. Liouville 1809～1882)才把伽罗华的数学遗稿汇集起来刊印在他自己创办的《数学杂志》上，人们才开始了解到这些科学成果的重要性。其中最重要的一篇的题目是《论方程可以用开方法求解的条件》。年纪不满二十一岁、大学还没有毕业的法国青年数学家的这篇论文是近代代数学发展进程中的一项重要成就。1870年，也就是伽罗华死后三十八年，法国数学家若当(C. Jordan 1838～1922)根据伽罗华的思想写了一本大书《论置换与代数方程》。在这本书里伽罗华的思想得到了进一步的阐述。到现在，阿贝尔、伽罗华最先提出的基本概念：置换群和群，已经发展成代数学的一个重要分支——群论。群论不仅对近代数学的各个方面，而且对物理、化学的许多分支都产生了重大的影响。

关于阿贝尔、伽罗华的方法及有关知识，我们放在本书的三、四、五介绍。

二、用根的置换理论解代数方程

上面我们利用作代换、配完全平方等方法找到了二、三、四次方程的代数求解公式。但这些方法有很大的局限性，解次数不同的方程要重起炉灶，似乎没有什么普遍的规律性，循着这样的途径去解五次方程，只能是挖空心思硬凑。一种方法失败了再换另一种方法试试。但即使试来试去总是失败，也不能说代数解法不存在。这也就是拉格朗日以前的数学家所走过的道路。

从拉格朗日开始，问题的本质比较清楚了. 他将前人各种求解代数方程的方法用根的置换理论统一起来，看清楚这些解法原来都是遵循着同一个基本原理的. 可是这一原理应用于解五次方程时却失败了. 正是这样，拉格朗日才开始认识到一般五次方程的代数解法很可能是不存在的.

下面我们首先来介绍如何用根的置换理论来解二、三、四次方程，然后用置换理论来阐明各种不同的解法所共同遵循的基本原理，最后指明这一原理为什么在解五次(或高于五次)方程时就失败了.

1. 利用根的置换解二次方程

先从大家熟悉的二次方程谈起，方程

$$x^2+px+q=0$$

有两个根 x_1 与 x_2. 而且根与方程系数之间有关系

$$x_1+x_2=-p,\ x_1x_2=q.$$

这两个关于根的多项式有一个重要的性质：将 x_1 换作 x_2、x_2 换作 x_1 $\left(\text{以后将这种根的置换方法记为}\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}\right)$，这两个多项式是不变的. 我们将这种置换的作用记为：

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}: x_1+x_2 \Longrightarrow x_2+x_1,$$

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}: x_1x_2 \Longrightarrow x_2x_1.$$

具有这种性质的多项式称为根的对称多项式，简称为对称多项式. 又如 $x_1^2+x_2^2$，$(x_1-x_2)^2$ 等等都是对称多项式. 但 x_1+2x_2，

x_1, x_1-x_2 等等就不是对称多项式. 例如

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}: x_1+2x_2 \Rightarrow x_2+2x_1 \neq x_1+2x_2.$$

在关于根 x_1, x_2 的对称多项式中以 x_1+x_2 与 x_1x_2 为最简单,它们被称为基本对称多项式,且分别等于 $-p$ 和 q. 可以证明

定理 任何关于根 x_1 与 x_2 的对称多项式, 必可用基本对称多项式 x_1+x_2, x_1x_2 的多项式表出, 也就是说, 可以用方程的系数 p, q 的多项式表出.

这条定理的证明是不难的, 但有些繁琐, 有兴趣的同志可以在高等代数的书本中找到它的证明. 我们在这里就把证明省略了. 下面只是举几个例子来说明一下(当然举例不能算是证明!).

[例] 我们已经知道 $(x_1-x_2)^2$ 和 $x_1^3+x_2^3$ 都是对称多项式,现在把它表为 x_1+x_2 和 x_1x_2 或者说 p, q 的多项式:

$$(x_1-x_2)^2 = x_1^2+x_2^2-2x_1x_2 = (x_1+x_2)^2-4x_1x_2 = p^2-4q,$$

$$x_1^3+x_2^3 = (x_1+x_2)^3-3x_1^2x_2-3x_1x_2^2 = (x_1+x_2)^3$$
$$-3x_1x_2(x_1+x_2) = -p^3+3pq.$$

利用上面的定理以及对称多项式的特点, 就可以求得二次方程的解. 事实上已经知道 $x_1+x_2=-p$, 若再能知道 x_1-x_2 等于什么,那就很容易求得 x_1 与 x_2 了. x_1-x_2 若是对称多项式问题就好办(因这时根据上面的定理,可把 x_1-x_2 表示成已知数 p, q 的多项式,就等于求出了 x_1-x_2). 可惜它不是对称多项式,因为

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}: x_1-x_2 \Rightarrow x_2-x_1 = -(x_1-x_2).$$

但是从上面置换的结果容易想到 $(x_1-x_2)^2$ 应该是对称多项

式：

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}:(x_1-x_2)^2 \Rightarrow (x_2-x_1)^2=(x_1-x_2)^2.$$

因为$(x_1-x_2)^2$是对称多项式，所以可以用 p, q 的多项式表示．事实上我们已求得过 $(x_1-x_2)^2=p^2-4q$，因此很容易得到 $x_1-x_2=\pm\sqrt{p^2-4q}$，利用

$$x_1+x_2=-p,$$
$$x_1-x_2=\pm\sqrt{p^2-4q},$$

立即可求得：

$$\begin{cases} x_1=\frac{1}{2}(-p+\sqrt{p^3-4q}), \\ x_2=\frac{1}{2}(-p-\sqrt{p^2-4q}). \end{cases}$$

这就是通常解二次方程的公式．

上面解二次方程的方法虽然没有提出什么新的结果（用通常配方的方法似乎比这里还简单一些）．但它却显示了解代数方程的一种普遍方法．因而循着这种方法的思路就容易得到解三、四次方程的公式．

2. 利用根的置换解三、四次方程

上面利用了根的多项式在根的置换作用下所发生的变化来求解二次方程，现在我们遵循同样的途径来求解三、四次方程．

先看三次方程

$$x^3+px^2+qx+r=0. \tag{2.1}$$

设 x_1, x_2, x_3 是它的三个根、则由韦达定理已知

$$
\begin{cases}
x_1+x_2+x_3=-p, \\
x_1x_2+x_2x_3+x_3x_1=q, \\
x_1x_2x_3=-r.
\end{cases}
\tag{2.2}
$$

$x_1+x_2+x_3$, $x_1x_2+x_2x_3+x_3x_1$, $x_1x_2x_3$ 这三个关于 x_1, x_2, x_3 的多项式具有这样的特点：它在对 x_1, x_2, x_3 的任何一种置换下都是不变的．根据排列的知识，可知这种置换共有 6 种：

$$
\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},
$$

$$
\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}
\tag{2.3}
$$

这里我们将置换

$$
\begin{pmatrix}x_1&x_2&x_3\\x_1&x_2&x_3\end{pmatrix},\ \begin{pmatrix}x_1&x_2&x_3\\x_1&x_3&x_2\end{pmatrix}\cdots
$$

等省去 x 保留下标，简记为

$$
\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdots,
$$

并将"不变"：

$$
\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}
$$

也算作一种置换，称为**恒等置换**．同样，我们把在上面 6 种置换作用下都不变的多项式称为**对称多项式**．例如

$$
x_1^2+x_2^2+x_3^2,\quad x_1^3+x_2^3+x_3^3,
$$

$$
x_1^2x_2+x_1x_2^2+x_2^2x_3+x_2x_3^2+x_3^2x_1+x_3x_1^2
$$

等都是对称多项式，读者可以自己验证一下．特别是(2.2)式中

$$
x_1+x_2+x_3,\ x_1x_2+x_2x_3+x_3x_1,\ x_1x_2x_3
$$

称为**基本对称多项式**．

同样可以证明：

定理 任何关于根 x_1, x_2, x_3 的对称多项式，必可用基本对称多项式(2.2)的多项式表示，也就是说，可用方程的系数 p, q, r 的多项式表出.

这个定理的证明我们也从略．而只是用一些例子说明.

［例］ 把 $x_1^2+x_2^2+x_3^2$ 用 p、q、r 的多项式表示出来.

$$
\begin{aligned}
x_1^2+x_2^2+x_3^2 &= (x_1+x_2+x_3)^2-2(x_1x_2+x_2x_3+x_3x_1) \\
&= p^2-2q,
\end{aligned}
$$

$$
\begin{aligned}
&x_1^2x_2+x_1x_2^2+x_2^2x_3+x_2x_3^2+x_3^2x_1+x_3x_1^2 \\
&= (x_1+x_2+x_3)(x_1x_2+x_2x_3+x_3x_1)-3x_1x_2x_3 \\
&= -pq+3r.
\end{aligned}
$$

现在就可以来讨论三次方程的求解问题了.

我们已看到在解二次方程时起关键作用的是多项式 x_1-x_2. 这里 x_1 与 x_2 的系数是 1 与 -1，它们恰恰是方程 $x^2-1=0$ 的两个根．因此联想到，在解三次方程时与之相当的应该是方程 $x^3-1=0$ 的三个根．已经说过方程 $x^3-1=0$ 的三个根记为 1, ω, ω^2，于是与解二次方程中起关键作用的多项式 x_1-x_2 相当的应该是多项式：

$$\psi_1=x_1+\omega x_2+\omega^2x_3. \tag{2.4}$$

ψ_1 也不是对称多项式．在 6 种置换

$$
\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},
$$
$$
\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},
$$
$$
\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}
$$

作用下 ψ_1 分别变为：

$$
\begin{aligned}
&\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}:\psi_1\Rightarrow x_1+\omega x_2+\omega^2x_3=\psi_1,\\
&\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}:\psi_1\Rightarrow x_1+\omega x_3+\omega^2x_2=\psi_2,\\
&\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}:\psi_1\Rightarrow x_2+\omega x_3+\omega^2x_1=\psi_3,\\
&\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}:\psi_1\Rightarrow x_2+\omega x_1+\omega^2x_3=\psi_4,\\
&\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}:\psi_1\Rightarrow x_3+\omega x_2+\omega^2x_1=\psi_5,\\
&\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}:\psi_1\Rightarrow x_3+\omega x_1+\omega^2x_2=\psi_6.
\end{aligned}
\tag{2.5}
$$

我们首先指出，x_1，x_2，x_3 可以用 p，ψ_1，ψ_2 等表示出来．例如，因为

$$
\begin{aligned}
-p+\psi_1+\psi_2&=(x_1+x_2+x_3)+(x_1+\omega x_2+\omega^2x_3)\\
&\quad+(x_1+\omega^2x_2+\omega x_3)\\
&=3x_1+(1+\omega+\omega^2)x_2+(1+\omega+\omega^2)x_3=3x_1,
\end{aligned}
$$

所以

$$x_1=\frac{1}{3}(-p+\psi_1+\psi_2), \tag{2.6}$$

用类似于(2.6)那样的式子，可得

$$x_2=\frac{1}{3}(-p+\omega^2\psi_1+\omega\psi_2), \tag{2.7}$$

$$x_3=\frac{1}{3}(-p+\omega\psi_1+\omega^2\psi_2). \tag{2.8}$$

从(2.6)～(2.8)看出，要是 ψ_1、ψ_2 的值能够求出，x_1、x_2、x_3 就能求出来了．于是问题转化为求 ψ_1、ψ_2．

如果 ψ_1、ψ_2 是 x_1、x_2、x_3 的对称多项式，那么只要根据定理把它们表示成 p、q、r 的多项式，就求出了 ψ_1、ψ_2 的值．但

遗憾的是它们不是对称多项式，我们只好把问题扩展一下.

不仅 ψ_1，而且 ψ_2、ψ_3、ψ_4、ψ_5、ψ_6 中的任一个在 6 种置换下的结果，都分别是 ψ_1、ψ_2、ψ_3、ψ_4、ψ_5、ψ_6 的某个次序的排列. 这就是说，在 6 种置换下，下述关于 t 的方程

$$(t-\psi_1)(t-\psi_2)(t-\psi_3)(t-\psi_4)(t-\psi_5)(t-\psi_6)=0 \quad (2.9)$$

总是不变的(因为任何一种置换作用于此方程的结果，不过是将其因子的次序重新排列一下而已). 这样一来，(2.9) 中的系数必定都是对称多项式，因而都可用 p、q、r 的多项式表示出来. 或者说，(2.9) 中的系数是已知的. 我们希望能从方程 (2.9) 中解出 ψ_1, ψ_2. (2.9) 虽然是 t 的六次方程，但是巧得很，由(2.5)知

$$\begin{aligned}&\psi_6=\omega\psi_1,\ \psi_3=\omega^2\psi_1,\\&\psi_4=\omega\psi_2,\ \psi_5=\omega^2\psi_2.\end{aligned} \quad (2.10)$$

所以

$$\begin{aligned}(t-\psi_1)(t-\psi_6)(t-\psi_3)&=(t-\psi_1)(t-\omega\psi_1)(t-\omega^2\psi_1)\\&=t^3-(\omega^2+\omega+1)\psi_1t^2+(\omega^2+\omega+1)\psi_1^2t-\psi_1^3\\&=t^3-\psi_1^3,\end{aligned}$$

同样 $$(t-\psi_2)(t-\psi_4)(t-\psi_5)=t^3-\psi_2^3.$$

于是方程(2.9)就成为

$$(t^3-\psi_1^3)(t^3-\psi_2^3)=0$$

或 $$t^6-(\psi_1^3+\psi_2^3)t^3+\psi_1^3\psi_2^3=0. \quad (2.11)$$

一方面方程(2.11)应仍和(2.9)一样，其系数是 p、q、r 的多项式，是已知的. 实际上可以求出

$$\begin{aligned}\psi_1^3+\psi_2^3&=-2p^3+9pq-27r,\\\psi_1^3\psi_2^3&=(p^2-3q)^3.\end{aligned}$$

另一方面，(2.11)实际上可以化成二次方程解，这只要把 t^3 看成一个元，从(2.11)即可解得

$$t^3=\frac{\psi_1^3+\psi_2^3\pm\sqrt{(\psi_1^3+\psi_2^3)^2-4\psi_1^3\psi_2^3}}{2}$$

$$=\frac{-2p^3+9pq-27r\pm\sqrt{(-2p^3+9pq-27r)^2-4(p^2-3q)^3}}{2}.$$

知道了 t^3 即易求得 t，即得方程 (2.9) 之 6 个根 ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, ψ_6. 知道了 ψ_1 与 ψ_2 再根据(2.8)即可求得原来三次方程的三个根 x_1, x_2, x_3. 这样，三次方程的求解问题就完全解决了.

现在来讨论四次方程的求解问题. 考察四次方程

$$x^4+ax^3+bx^2+cx+d=0, \tag{2.12}$$

它的四个根记为 x_1, x_2, x_3 与 x_4，它们与方程式的系数之间有下列关系(韦达定理)：

$$\begin{cases} x_1+x_2+x_3+x_4=-a, \\ x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4=b, \\ x_1x_2x_3+x_1x_2x_4+x_2x_3x_4+x_1x_3x_4=-c, \\ x_1x_2x_3x_4=d. \end{cases} \tag{2.13}$$

由排列理论知道四个根 x_1, x_2, x_3, x_4 的各种置换共有 $4!=24$ 种(包括恒等置换)：

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\cdots \tag{2.14}$$

基本对称多项式与对称多项式的概念与二、三次方程的情况完全类似，同样也有

定理 任何关于根 x_1, x_2, x_3, x_4 的对称多项式可用基本对称多项式的多项式表出，也就是说可用方程的系数 a, b, c, d 的多项式表出.

方程 $x^4-1=0$ 的四个根是 1, -1, i, $-i$. 因此与解三次方程时所引进的根的多项式 $\psi_1=x_1+\omega x_2+\omega^2 x_3$ 相当的根的多项式应该是 $\phi_1=x_1-x_2+ix_3-ix_4$, 但这样做下去变化很多, 比较麻烦. 我们另外研究类似的多项式:

$$V_1=x_1+x_2-x_3-x_4 \tag{2.15}$$

在(2.14)的 24 种置换作用下, V_1 的变化共有下面 6 种形式:

$$\begin{cases} V_1=x_1+x_2-x_3-x_4, \\ V_2=-x_1-x_2+x_3+x_4=-V_1, \\ V_3=x_1+x_3-x_2-x_4, \\ V_4=-x_1-x_3+x_2+x_4=-V_3, \\ V_5=x_1+x_4-x_2-x_3, \\ V_6=-x_1-x_4+x_2+x_3=-V_5. \end{cases} \tag{2.16}$$

因此, 一方面方程

$$(t-V_1)(t-V_2)(t-V_3)(t-V_4)(t-V_5)(t-V_6)=0 \tag{2.17}$$

在 24 种置换作用下不变, 故(2.17)展开后其系数是根的对称多项式, 因而可用 a, b, c, d 的多项式表出. 或者说(2.17)是系数已知的方程. 另一方面, 由(2.16)可知此方程又可化为:

$$(t^2-V_1^2)(t^2-V_3^2)(t^2-V_5^2)=0, \tag{2.18}$$

所以它是 t^2 的三次方程. 而三次方程我们已经会解了, 在解得 t^2 后, 利用开方即可求得(2.17)的 6 个根 V_1, V_2, V_3, V_4, V_5, V_6. 利用

$$\begin{cases} V_1=x_1+x_2-x_3-x_4, \\ V_3=x_1+x_3-x_2-x_4, \\ V_5=x_1+x_4-x_2-x_3, \\ -a=x_1+x_2+x_3+x_4. \end{cases} \tag{2.19}$$

即可解得

$$\begin{cases} x_1 = \frac{1}{4}(V_1+V_3+V_5-a), \\ x_2 = \frac{1}{4}(V_1-V_3-V_5-a), \\ x_3 = \frac{1}{4}(-V_1+V_3-V_5-a), \\ x_4 = \frac{1}{4}(-V_1-V_3-V_5-a). \end{cases} \tag{2.20}$$

这样，我们就解决了四次方程的求解问题.

3. 一般五次(或五次以上)方程的代数求解问题

拉格朗日用置换的理论回过头来分析了卡当方法和费拉利方法，从中发现共同的原理.

先看卡当方法(见第5页). 卡当解法的关键一步是引进了代换

$$x = z - \frac{p}{3z}, \tag{2.21}$$

正是这个代换使得原来不能解的方程

$$x^3 + px + q = 0 \tag{2.22}$$

变成了可以解的方程

$$z^6 + qz^3 - \frac{p^3}{27} = 0. \tag{2.23}$$

或者说就可解与不可解这一点而言，(2.23)与(2.22)有本质不同. 但(2.23)又不是随便写出的，它的解 z 是由(2.22)的解 x 制约的. 拉格朗日精辟地指出：奥秘正是在这里，正是在于 z 到底是如何用 x 表示出来的. (2.21)式说的是 x 是 z 的函数，拉格朗日却指出我们不应该把注意力集中于此，而应该集中于 z 是 x 的什么样的函数这一点上.

拉格朗日发现，在下面这个关于 x_1, x_2, x_3 的多项式

$$\frac{1}{3}(x_1+\omega x_2+\omega^2 x_3) \tag{2.24}$$

中，把 x_1, x_2, x_3 作置换（回忆一下，共有六种置换），就可以得出(2.23)中 z 的六个解．这只要用

$$\begin{cases} x_1=u+v, \\ x_2=u\omega+v\omega^2, \\ x_3=u\omega^2+v\omega, \end{cases} \tag{2.25}$$

代到 6 种置换下的(2.24)式中，即得

$$u,\ u\omega,\ u\omega^2,\ v,\ v\omega,\ v\omega^2,$$

这正是(2.23)的解．于是拉格朗日找出了 z 与 x 的值的关系是在置换意义下的下式

$$z=\frac{1}{3}(x_1+\omega x_2+\omega^2 x_3).$$

上面说过，z 在 6 种置换下取六个不同的值，因此，z 不得不由一个六次方程决定．但是

$$z^3=\frac{1}{27}(x_1+\omega x_2+\omega^2 x_3)^3 \tag{2.26}$$

在 6 种置换下却只取两个值（理由正是我们在 24 页上说过的(2.10)式，读者可以自己想一想），从而 z^3 的确应该由一个二次方程确定出来．得出了 z，再由 $x=z-\frac{p}{3z}$ 求 x 就不难．

读者已经看到，方程的可解与不可解确实与置换很有关系．

再看费拉利法解四次方程（见 11 页）．为了凑成完全平方，关键在于引进了辅助未知量 t, t 满足的方程 (1.27) 是可解的．那么和前面一样，我们要问，t 和方程原来的根有什么关系呢？设方程 (1.29) 的两根为 x_1 与 x_2，方程(1.30) 的两根

为 x_3, x_4, 则易见

$$\begin{cases} x_1x_2 = \dfrac{t_0}{2} + \sqrt{\dfrac{t_0^2}{4} - d}, \\ x_3x_4 = \dfrac{t_0}{2} - \sqrt{\dfrac{t_0^2}{4} - d}, \end{cases} \tag{2.27}$$

两式相加即得 $t_0 = x_1x_2 + x_3x_4$,

而 $t_0 = x_1x_2 + x_3x_4$ 在 x_1, x_2, x_3, x_4 的 24 种置换作用下仅取三种不同的值, 因此它必满足一个系数为已知的三次方程(1.27), 从而是可解的. 得出了 t_0, 再求 x 就不难了.

所以不管是卡当法、费拉利法或拉格朗日法(其它方法也如此), 解三、四次方程的关键都在于引进一个关于原来的根的函数——一个恰当的辅助量 $\left(\text{如 } z = \dfrac{x_1 + \omega x_2 + \omega^2 x_3}{3},\ t = x_1x_2 + x_3x_4,\ V = x_1 + x_2 - x_3 - x_4 \text{ 等}\right)$, 这些辅助量是根的多项式, 用这些辅助量及其在置换下的不同的值, 往回可以求出原来的根. 往前看, 这些辅助量(或它的某次幂)又可以由一个次数较低的方程解出来, 这个方程的系数是原方程系数的多项式, 因而是已知的.

拉格朗日还更一般地研究了根的有理函数(即多项式之商, 多项式是有理函数之特例)与置换之间的关系. 他证明了两个重要的命题. 这构成了上述作法的理论根据.

命题一 如果使根的有理函数 $\psi(x_1, x_2, \cdots, x_n)$ 不变的一切置换也使根的另一有理函数 $\phi(x_1, x_2, \cdots, x_n)$ 不变, 则 ϕ 必可用 ψ 及原方程的系数 $a_0, a_1, \cdots, a_n$ 的有理函数表出.

命题二 如果使根的有理函数 $\phi(x_1, x_2, \cdots, x_n)$ 不变的置换亦使另一有理函数 $\psi(x_1, x_2, \cdots, x_n)$ 不变; 而且在使 $\psi(x_1, x_2, \cdots, x_n)$ 不变的所有置换作用下, ϕ 取 r 个不同的值, 则 ϕ

必满足一 r 次代数方程，其系数为 ψ 及原方程之系数 $a_0, a_1, \cdots, a_n$ 的有理函数。

这两个命题我们不打算给出证明，只是举几个例子说明一下。

先说命题一。

[例 1] 考察 $x^2+px+q=0$ 的根 x_1、x_2 的两个多项式

$$\phi=x_1 \quad 与 \quad \psi=x_1-x_2.$$

使 ψ 不变的置换只有恒等置换，当然也使 ϕ 不变. 由命题一知 ϕ 可以用 p、q 为系数的 ψ 的多项式表出. 事实上也确实有

$$\phi=x_1=\frac{x_1+x_2+(x_1-x_2)}{2}=\frac{-p+\psi}{2}.$$

[例 2] 考察 $x^3+px^2+qx+r=0$ 的根 x_1、x_2、x_3 的两个多项式

$$\phi=(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

与
$$\psi=(x_1+\omega x_2+\omega^2x_3)^3.$$

则所有使 ψ 不变的置换是

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

这三个置换也使 ϕ 不变. 因此由命题一知，ϕ 可以用 ψ 的以 p、q、r 为系数的多项式表出. 事实上，通过具体计算易知：

$$\phi=\frac{1}{3\sqrt{-3}}[2\psi+(2p^3-9pq+27r)]$$

另外，我们注意到使

$$\psi_1=x_1+\omega x_2+\omega^2x_3$$

不变的置换只有恒等置换，恒等置换当然使任何 x_1, x_2, x_3 的多项式不变，因而，关于 x_1、x_2、x_3 的任何多项式，都可用 ψ_1 的有理函数（以 p、q、r 为系数）表出. 特别地，x_1, x_2, x_3 也

是可表的，例如通过具体的计算易知：

$$x_1=\frac{1}{3}\left(-p+\psi_1+\frac{p^2-3q}{\psi_1}\right).$$

[例 3]　考察 $x^4+ax^3+bx^2+cx+d=0$ 的根的多项式

$$V=x_1+x_2-x_3-x_4$$

与

$$t=x_1x_2+x_3x_4.$$

使 V 不变的置换是

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$

$$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}.$$

这四个置换亦使 $t=x_1x_2+x_3x_4$ 不变．事实上

$$t=\frac{1}{4}(V^2-a^2+4b).$$

再说命题二的应用．

[例 4]　三次方程 $x^3+px^2+qx+r=0$ 的三个根 x_1, x_2, x_3 的有理函数 $\psi=x_1+x_2+x_3$ 在所有 6 种置换作用下都不变（因 ψ 是对称多项式），而 $\phi=(x_1+\omega x_2+\omega^2x_3)^3$ 在此 6 种置换作用下取两种不同的值（见(2.5)及(2.10)），所以由命题二知 ϕ 应满足一个二次方程，其系数为 ψ 及 p, q 的有理函数．事实上我们已知道 ϕ 满足下列二次方程：

$$\phi^2+(2p^3-9pq+27r)\phi+(p^2-3q)^3=0.$$

[例 5]　四次方程 $x^4+ax^3+bx^2+cx+d=0$ 的四个根 x_1, x_2, x_3, x_4 的有理函数 $\psi=x_1x_2+x_3x_4$，使之不变的所有置换为以下 8 个：

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},$$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$$

而这 8 个置换使

$$\phi=x_1+x_2-x_3-x_4.$$

取 2 种不同的值：$x_1+x_2-x_3-x_4$ 与 $x_3+x_4-x_1-x_2$. 所以 ϕ 满足一个二次方程，其系数为 ψ 及 a, b, c, d 之有理函数. 此方程如下：

$$\phi^2-(a^2-4b+4\psi)=0.$$

在得到了以上两个命题之后，拉格朗日拟订了一种解 n 次代数方程的方案(已知的一些代数求解方法，都可归结为这一方案的一种具体体现).

他的方案是这样的：

对一个 n 次代数方程先取一个根的对称多项式 ϕ_0, 它在所有 $n!$ 个置换作用下都不变. 根据韦达定理我们知道 ϕ_0 一定可用方程的系数的多项式表出. 为简单起见，不妨就取

$$\phi_0=x_1+x_2+x_3+\cdots+x_n.$$

然后再取一个根的多项式 ϕ_1, 设 ϕ_1 在 $n!$ 个置换作用下就不是不变了，而是取 r 种不同的值. 于是由命题二知道，ϕ_1 是一个 r 次方程的根，此方程的系数是由 ϕ_0 及原方程的系数的有理函数所构成. 若此 r 次方程可用代数方法求解，则 ϕ_1 就可用原方程的系数的代数式表出. 然后再取一根的多项式 ϕ_2, 使 ϕ_2 不变的置换仅为使 ϕ_1 不变的置换的一部分. 若使 ϕ_1 不变之全部置换作用于 ϕ_2 时得到 s 种不同的值，于是 ϕ_2 满

是一 s 次方程，其系数为 ϕ_1 及原方程系数的有理函数．若此 s 次方程可用代数方法求解，则显然 ϕ_2 就可用原方程的系数的代数式表出．如此，继续作出 ϕ_3，ϕ_4，…，因为使 ϕ_k 不变的置换随 k 增大而逐步减少．最后直至使 ϕ_k 不变之置换仅有恒等置换即可停止．这最后的 ϕ_k，不妨即可取 x_1．若上述过程中这些 r 次，s 次，…方程均可用代数方法求解，则 x_1 就可以用原方程的系数的代数式表出．当然 x_2，…，x_n 也可同样求得．这些 r 次，s 次，…方程就称为预解式．

因为在三、四次方程的情况，预解式的次数较已知方程的次数少一，所以三、四次方程可用代数方法求解．可是就五次方程而论，情况就完全不同了．拉格朗日发现他所得出的五次方程的预解式是一个六次方程了．他费了很多精力去寻找能导致次数低于五次方程的预解式，但始终没有成功．所以就五次方程而言，拉格朗日的方法就完全失掉了作用．拉格朗日虽然没有求出这样的预解式，但不能就此下结论说这种预解式不存在，更不能说一定没有其它代数求解的途径了．由上面的讨论只能说五次方程的代数解法很可能是不存在的．只有应用了伽罗华的理论，才能最终弄清解代数方程的原理，并严格证明一般五次方程不存在代数解法．

伽罗华理论需要一些预备知识，这些知识连同伽罗华理论及应用，就是我们下面所要介绍的．

三、置换群及其重要性质

上面我们已看到了根的置换理论在讨论代数方程求解方法中所起的重要作用．在这一章中我们要来进一步讨论置换

的一些重要性质，并引进置换群的概念，作为下面介绍伽罗华理论的准备。

1. 置换的乘积及其基本性质

我们已经介绍过置换的记号

$$\begin{pmatrix} 1 & 2\cdots n \\ \alpha_1 & \alpha_2\cdots\alpha_n \end{pmatrix},$$

这里 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 $1, 2, \cdots, n$ 的一种排列。这个记号表示将 x_1 换作 x_{α_1}，将 x_2 换作 x_{α_2}，$\cdots$，x_n 换作 x_{α_n} 这样一种置换。所以

$$\begin{pmatrix} 1 & 2\cdots n \\ \alpha_1 & \alpha_2\cdots\alpha_n \end{pmatrix} \quad 与 \quad \begin{pmatrix} 3 & 4 & 2 & 1 & 5 & 6\cdots n \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 & \alpha_5 & \alpha_6\cdots\alpha_n \end{pmatrix}$$

表示同一置换，也就是说置换的记号中列的次序毫无关系，关键在于每一列中上下两数字的关系要保持不变。例如

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad 与 \quad \begin{pmatrix} 3 & 2 & 4 & 1 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

或

$$\begin{pmatrix} 4 & 2 & 1 & 3 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

都表示同一置换，也就是说这几个记号都表示将 x_1 换为 x_4，x_2 换为 x_3，x_3 换为 x_2，x_4 换为 x_1 这个置换。

置换的乘积 设有两个置换

$$s=\begin{pmatrix} 1 & 2\cdots n \\ \alpha_1 & \alpha_2\cdots\alpha_n \end{pmatrix} \quad 与 \quad t=\begin{pmatrix} \alpha_1 & \alpha_2\cdots\alpha_n \\ \beta_1 & \beta_2\cdots\beta_n \end{pmatrix},$$

若对 n 个根 $x_1, \cdots, x_n$ 的多项式先施行置换 s 再施行置换 t，则与施行单单一个置换

$$u=\begin{pmatrix}1 & 2\cdots n\\ \beta_1 & \beta_2\cdots\beta_n\end{pmatrix}$$

之作用相同，我们称置换 u 为置换 s 与 t 的乘积，记为 $u=st$，例如

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}4&2&1&3\\3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}.$$

但要注意置换的乘法未必具有交换性，也就是说一般 st 与 ts 未必相等．例如在上例中

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},$$

但

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}2&1&4&3\\2&4&3&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}.$$

显然 $$\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\neq\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},$$

这是置换的乘法与普通乘法不同之处．

结合律 置换之乘法虽然未必具有可交换性，但却满足结合律，即对任意三个置换 s, t, v, 都有

$$(st)v=s(tv),$$

这从置换的定义是很容易验证的．我们只举例说明一下．

［例］ 设

$$s=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix},\ t=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},$$

$$v=\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},$$

则 $$st=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},$$

$$(st)v=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},$$

而 $$tv=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},$$

$$s(tv)=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}.$$

$$\therefore\quad (st)v=s(tv).$$

恒等置换 我们称

$$\begin{pmatrix}1&2&3\cdots n\\1&2&3\cdots n\end{pmatrix}$$

为恒等置换，以后常把这个置换记为 I.

逆置换 对任何置换

$$s=\begin{pmatrix}1&2\cdots n\\\alpha_1&\alpha_2\cdots\alpha_n\end{pmatrix},$$

必有一相应的置换 s' 使 $ss'=s's=I$. 显然此置换必为

$$s'=\begin{pmatrix}\alpha_1&\alpha_2\cdots\alpha_n\\1&2\cdots n\end{pmatrix},$$

我们称此置换为 s 之逆置换，以后记作 s^{-1}. 所以

$$ss^{-1}=s^{-1}s=I,$$

且 $$(s^{-1})^{-1}=s,$$

2. 置换群的概念

我们已经知道：所谓根的对称多项式就是在所有 $n!$ 种置换作用下都是不变的多项式．而非对称多项式就是指在有些置换下会变化的多项式．以 $n=3$ 为例，多项式

$$\phi=(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

在所有 $3!=6$ 种置换作用下，有的置换会使它发生变化，例如

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}:\phi\Rightarrow(x_2-x_1)(x_1-x_3)(x_3-x_2)=-\phi,$$

但有的却不会使它发生变化，例如

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}:\phi\Rightarrow(x_2-x_3)(x_3-x_1)(x_1-x_2)=\phi.$$

我们将所有使 ϕ 不发生变化的置换全部拿来，共有以下 3 个：

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad b=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

我们来研究一下由这三个置换 I, a, b 所组成的集合 G 的一些重要性质：

对这个集合中的任意两个元素（置换），我们已经定义了一种乘法——置换的乘法．容易验证

$$Ia=aI=a,\ Ib=bI=b$$

及
$$ab=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=I=ba,$$

$$aa=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=b,$$

$$bb=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=a.$$

这里我们看到了一个现象：任取 G 中两元素，它们的乘积仍为 G 中的元素；而且 G 中每一置换之逆置换亦在 G 中（$I^{-1}=I$, $a^{-1}=b$, $b^{-1}=a$）. 当然，从所有置换中随便取一部分出来组成一个集，未必一定会有上述性质的. 我们把集 G 所具有的这种特殊性质一般地叙述一下，就是

(1) 对 G 中任意两个置换规定了一种运算——置换的乘积 G 中的置换经过这一运算后，所得的结果仍是 G 中的一个置换；

(2) 这种运算是满足结合律的；

(3) G 中含有恒等置换，它与 G 中任何置换运算的结果仍是那个置换；

(4) G 中的每一置换在 G 中必有一逆置换.

一些置换所组成的集合，如果能满足以上四条性质，我们就称此集合为一*置换群*. 上面例子中 I, a, b 三置换所组成的集合 G 就构成一置换群.

我们说过，并不是所有由置换构成的集合一定会是置换群. 注意上述 G 的特殊之处是 G 恰好是使一个多项式

$$(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

不变的所有那些置换组成的. 这一点并非偶然. 事实上对 $x_1, x_2, \cdots, x_n$ 的任意一个多项式 $\psi(x_1, \cdots, x_n)$ 来说，使它不变的所有置换构成的集 H 必定是一个置换群. 这是因为若置换 s 与 t 均使 ψ 不变的话，则 s 与 t 之乘积对 ψ 所起的作用，不过是将 s 与 t 这两置换相继作用于 ψ 而已. 所以 st 亦必然使 ψ 不变. 也就是说由 s, t 属于 H 必可推出 st 亦属于 H. 因此 H 满足(1)；至于性质(2)则是对任意置换的乘

积都满足的，H 中的置换当然也不例外，故不必另行验证；因恒等变换 I 当然不会使 ψ 发生变化，所以 I 在 H 中，即性质(3)也是满足的；最后如果某一置换 s 使 ψ 不变，而 s^{-1} 却使 ψ 发生变化，则 $ss^{-1}=I$ 会使 ψ 发生变化，这显然与 I 的定义矛盾的，这说明 s^{-1} 必然也使 ψ 不变，故性质(4)亦满足．总之，这就证明了使某一多项式 $\psi(x_1, \cdots, x_n)$(或有理函数)不变的置换全体构成一置换群．

［例］ 使 $V=x_1+x_2-x_3-x_4$ 不变的置换共有以下四个置换：

$$I=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad a=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},$$

$$b=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\quad c=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$

I, a, b, c 也构成一个置换群．

反过来，我们可以证明：给定了一个置换群 G 后，必能求得一多项式 $t(x_1, \cdots, x_n)$，而使 $t(x_1, \cdots, x_n)$ 不变的置换全体恰恰就是 G，具体的证明这里就不写了．

3．一般的群的概念

把上面引进的置换群的概念再加以抽象推广，就形成了一般的群的概念．上节介绍的置换群，不过是一种特殊的群．群是近代数学中最重要的概念之一．它不仅对数学的许多分支都有着深刻的影响，而且在近代的物理、化学中也有许多重要的应用．我们在这里简单介绍一下这个概念．

任意一个集合，它的元素可以是数(比如说实数集)，也可以不是数(比如说以置换为元素的集合)．元素的个数可以是

有限个，也可以是无限个. 在这个集合中对任意两个元素往往可以规定一种运算(有时可以有不止一种运算，但我们这里只需要因而也只允许考察一种运算)，这种运算也是多种多样的.

[例] (i) 元素为一切整数所成之集合，运算为加法；

(ii) 元素为一切不等于 0 的实数所成之集合，运算为乘乘法；

(iii) 元素为一切不等于 0 的有理数所成之集合，运算为法；

(iv) 元素为 1, -1, i, $-i$ 四个数所成之集合，运算为乘法；

(v) 元素为 n 个文字的全部(共 $n!$ 个)置换：

$$\begin{pmatrix} 1 & 2 \cdots n \\ \alpha_1 & \alpha_2 \cdots \alpha_n \end{pmatrix},$$

运算为前面定义过的置换的乘积；

(vi) 元素是正六角形绕原点的旋转，旋转的角度是 60° 或 60° 的倍数(这种旋转共有 60°, 120°, 180°, 240°, 300°, 360° 六个)，运算为将一个旋转紧接着另一个旋转(而进行).

规定了一种运算的集合，若满足以下(1)～(4)这四条性质就称为一个**群**. 以后用大写字母 G, H, K 等记群，小写字母 g, h, …等记群的元素. 上述(i)～(vi)中的集合都是群. 我们边叙述性质边验证它们是群.

(1) 若集合中任意两个元素经过那规定的运算后，所得的结果还是集合中的一元素；例如

(i) 中两整数相加的结果还是整数；

(ii) 中两不等于 0 的实数相乘的结果还是不等于 0 的实数；

(iii) 中两不等于 0 的有理数相乘的结果还是不等于 0 的有理数;

(iv) 中 1, -1, i, $-i$ 任意取两数相乘结果还是这四个数之一;

(v) 中任意两置换之乘积仍为一置换;

(vi) 中角度为 60° 倍数的一个旋转跟着另一个旋转，结果还是一个角度为 60° 倍数的旋转.

所以集合(i), (ii), (iii), (iv), (v), (vi) 对相应规定的运算都满足性质(1).

(2) 集合中含有恒等元素(通常记为 I)，它与集合中任一元素运算后的结果仍是该元素; 例如

(i) 中恒等元就是 0, 0 加上任何整数 z 仍得该整数 z;

(ii) 中恒等元就是 1, 1 乘上任何实数 $r(\neq 0)$ 后仍得该实数 r;

(iii) 中恒等元就是 1, 1 乘上任何有理数 $q(\neq 0)$ 后仍得该实数 q;

(iv) 中恒等元就是 1, 1 乘上 -1, i, $-i$ 中的任一个后仍得该数;

(v) 中恒等元就是恒等置换

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

它与任何置换 a 相乘后仍得置换 a;

(vi) 中恒等元就是转角为 360° 的旋转; 它接在任何旋转之前(或之后)不改变这个旋转的作用.

(3) 集合中每一元素有一逆元素，元素与逆元素运算的结果等于恒等元素，以后记元素 g 的逆元素为 g^{-1}; 例如

(i) 中任一整数 m 的逆元素就是 $-m$;

(ii) 中任一不等于 0 的实数 x 的逆元素就是 $\frac{1}{x}$;

(iii) 中任一不等于 0 的有理数 r 的逆元素就是 $\frac{1}{r}$;

(iv) 中 -1 的逆元素是 -1, i 的逆元素是 $-i$, $-i$ 的逆元素是 i;

(v) 中置换 $\begin{pmatrix} 1 & 2 \cdots n \\ \alpha_1 & \alpha_2 \cdots \alpha_n \end{pmatrix}$ 的逆元素是置换 $\begin{pmatrix} \alpha_1 \cdots \alpha_n \\ 1 \cdots n \end{pmatrix}$;

(vi) 中 α° 旋转的逆元素是 $360^\circ-\alpha^\circ$ 的旋转.

读者可以分别验证一下，这些逆元素与原来元素的乘积确实为相应集合中的恒等元.

(4) 集合中规定的运算满足结合律.

设 a, b, c 是集合中任意三个元素，运算用记号$\circ$来表示，那末结合律就是说 $(a\circ b)\circ c=a\circ(b\circ c)$; (i) ～(vi) 中规定的运算显然都满足结合律，读者可以自己进行证明.

由此可见(i)～(vi) 中的集合对相应规定的运算确实都成为群.

上面这样不厌其详地进行验证，目的是为了说明群的运算的多样性以及在多样性背后的共同本质. 但为了方便起见，今后不管群中元素之间的运算具体是什么样的，都把它称为乘法. 并记为 $g\circ h$ 或 gh.

群的元素可以是有限个（如例(iv)，(v)，(vi)），这时称为**有限群**，也可以是无限个(例如(i)，(ii)，(iii))，这时称为**无限群**. 下面我们讨论的群都是有限群.

群中元素的乘法一般不满足交换律（即一般 $a\circ b\neq b\circ a$). 若除了以上四条性质，乘法还满足交换律的话，这时的群就叫做**交换群**或**阿贝尔(Abel)群**. 例(i)，(ii)，(iii)，(iv)，(vi)都是阿贝尔群，而(v)则不是阿贝尔群.

带有一个运算的集合并不都是群．作为例子，容易验证自然数全体对通常的加法运算不成为群(因为这时没有恒等元素，也没有逆元素)。全体实数对普通的乘法运算也不成为群(因为0这个元素没有逆元素)．

4. 群的重要性质

这一部分内容尽管并不难懂，但第一次接触的读者可能会感到抽象．然而这些却是了解伽罗华理论所必需掌握的．要是有些概念在第一次接触时感到较难理解，还可以在以后几章用到时回过来重读．另外，这部分内容虽然主要都以具体的置换群为例，但所有的概念和性质对一般的群都是成立的．

群的阶数　有限群的元素的个数称为这个群的阶数．

我们已经知道 n 个文字的全体置换 (共 $n!$ 个) 构成一个群，我们称这个群为*对称群*，以后记为 S_n．显然对称群 S_n 的阶数为 $n!$．

子群　一个群 G 的一部分元素 H 如果对于群 G 的运算也构成一个群，则称 H 是 G 的一个*子群*．

[例1]　对称群 S_3:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

我们已经知道其中三个置换(记为 A_3):

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

也成为一个群，所以这三个置换所构成的群 A_3 是 S_3 的一个子群.

[例 2]　全体整数对加法运算所成的群中，偶数全体是它的一个子群. 但是奇数全体就不成为群了(为什么?). 这说明并不是群中的任意一部分元素都能构成子群.

再来举一个重要的子群的例子:

[例 3]　我们已知上面例子中 S_3 的子群 A_3 使多项式 $\phi=(x_1-x_2)(x_2-x_3)(x_3-x_1)$ 不变. 一般地，我们来考察

$$\phi(x_1, \cdots, x_n)$$
$$=(x_1-x_2)\cdots(x_1-x_n)(x_2-x_3)\cdots(x_2-x_n)\cdots(x_{n-1}-x_n).$$

这个多项式也就是所有 (x_i-x_j), $(i<j)$, 形式的因子的乘积. 将 S_n 中任一置换 S 作用于 ϕ 时，显然有

$$S: \phi(x_1, \cdots, x_n) \Rightarrow \pm\phi(x_1, \cdots, x_n),$$

如果 $S: \phi\Rightarrow+\phi$, 则称 S 是偶置换，若 $S: \phi\Rightarrow-\phi$, 则称 S 是奇置换. 在 $n=3$ 即 S_3 的情况,

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

都是偶置换，而

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

都是奇置换.

不难证明 S_n 的全体偶置换是 S_n 的一个子群，记为 A_n, 我们称 A_n 为交代群. 因为 S_n 中的置换不是奇置换就是偶置换. 而全体偶置换用某一奇置换右乘后就变成全体奇置换. 因此 S_n 中偶置换的个数必等于奇置换的个数，也就等于全体置换的个数($=n!$)的一半，所以 A_n 的阶数为 $\frac{n!}{2}$.

另外，对一个群 G，仅由其恒等元素 I 所组成的集合显然是 G 的一个子群．群 G 本身也可以看成是 G 的一个子群．这两个特殊的子群称为 G 的**平凡子群**，其它的子群则称为**非平凡子群**．

关于群和它的子群的阶数之间有下列关系：

定理 群的阶数必能被其子群的阶数所整除，或者说子群的阶数是群的阶数的因子．

证明 设群 G 有 n 个元素．H 是它的一个子群，设有 r 个不同元素，记为 $g_1, g_2, \cdots, g_r$．我们任取一个不在 H 中的 G 的元素 a，作出 r 个乘积如下．

$$g_1a,\ g_2a,\ \cdots,\ g_ra$$

这 r 个元素都相异（如果有 $g_sa=g_ta$，则两边乘 a^{-1} 就有 $g_s=g_t$，与 g_s、g_t 相异的假设矛盾），而且都在 G 中，但都不属于 H（否则 a 要属于 H 了）．如 $n>2r$，我们一定还可以取一个 G 中的元素 b，b 与以上所得的 $2r$ 个元素相异，于是再作

$$g_1b,\ g_2b,\ \cdots,\ g_rb.$$

这 r 个元素都相异，而且在 G 中，但与以前的 $2r$ 个元素都相异．因此，G 中的 n 个元素可以排成下列形式：

$$\begin{gathered} g_1,\ g_2,\ \cdots,\ g_r, \\ g_1a,\ g_2a,\ \cdots,\ g_ra, \\ g_1b,\ g_2b,\ \cdots,\ g_rb, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots. \end{gathered}$$

所以 r 必能除尽 n.

循环群 若一群的所有元素均由其某一元素的连乘积（乘幂）所构成，则称此群为**循环群**．如果这个元素记成 S，可以证明循环群 G 一定可写成：

$$G=\{I,\ S,\ S^2,\ \cdots,\ S^{n-1}\}.$$

其中 $I=S^n$.

[例 1] 群 A_3 由三个置换

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ S=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ t=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

组成，但

$$t=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=S^2,$$

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$=S^3,$$

所以 A_3 是循环群，且

$$A=\{I,\ S,\ S^2\}.$$

[例 2] 群 G 由六个置换

$$I=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix},\quad a=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},$$

$$b=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix},\quad c=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix},$$

$$d=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix},\quad e=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$$

所组成，读者可以验证 $b=a^2$, $c=a^3$, $d=a^4$, $e=a^5$, $I=a^6$. 所以 G 也是一循环群，且

$$G=\{I,\ a,\ a^2,\ a^3,\ a^4,\ a^5\}.$$

周期 设群 G 的阶数为 n，在 G 中任取一元素 S，作 S 的乘幂

$$S,\ S\cdot S=S^2,\ S\cdot S\cdot S=S^3,\ \cdots,\ S^{n+1},$$

则由群之性质知这些乘幂都为 G 之元素. 但 G 的元素仅有 n 个，所以这 $n+1$ 个乘幂中必有相同者.

设 $$S^m=S^{m+p},\quad (m,\ p \text{ 为某二正整数})$$
取 S^m 之逆元 $(S^m)^{-1}$ 左乘上式二端得
$$(S^m)^{-1}\cdot S^m=(S^m)^{-1}\cdot S^m\cdot S^p,$$
即 $$I=I\cdot S^p,\ \text{或}\quad I=S^p.$$
所以对 G 中任何元素 S 一定存在正整数 p 使 $S^p=I$. 现取能使 $S^p=I$ 的那些 p 中最小的一个正整数 σ，称为元素 S 之周期. 各个元素的周期未必相同. 特别地，元素 I 而且仅有这个元素的周期恒为 1.

显然，I, S, S^2, $\cdots$, $S^{\sigma-1}$ 构成一 σ 阶子群，这个子群是一个循环子群，所以由上面的定理知，一个群的阶数必能被其任一元素的周期整除. 由此即可得一重要推论：

推论 若群 G 之阶数 n 为一素数，则 G 必为一循环群.

这是由于：任取 G 中一个元素 $S\neq I$. 因为 n 是素数，则其因子只有 1 和 n. 因为 $S\neq I$，故周期 $\neq 1$. 从而 S 之周期必等于 n. 于是由 S 之乘幂所构成的循环群 I, S, S^2, $\cdots$, S^{n-1} 恰有 n 个元素，正好穷尽 G 的所有元素. 这说明
$$G=\{I,\ S,\ S^2,\ \cdots,\ S^{n-1}\},$$
即 G 是循环群.

在伽罗华理论中占特别重要地位的是一种特殊的子群——不变子群，为了说清楚什么是不变子群. 我们先来解释一下变形的意义.

设有一群 G，h 与 g 为 G 中两元素，则用 h 右乘 g，再用 h 之逆元素左乘，所得的结果称为用 h 将 g 作变形. 即利用 h 将 g 变为 $h^{-1}gh$. 例如在群 S_3 中取
$$g=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad h=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

则
$$h^{-1}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix},$$

$$h^{-1}gh=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},$$

所以$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$用$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$变形之结果为$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$.

读者容易看出$hg=gh$和$h^{-1}gh=g$是一回事. 因为群中元素的乘法一般不满足交换律，所以通常$h^{-1}gh\neq g$，即一个元素经变形之后通常不等于原来的元素. 但对阿贝尔群(交换群)则恒有$h^{-1}gh=h^{-1}hg=g$，这时变形之后仍变成自己. 因此变形的概念就没有什么意义了.

不变子群 设H是G的一个子群，若H中任一元素用G中任一元素加以变形，所得到的元素仍为H中之元素，则称H是G的不变子群.

[例1] 交代群A_3:

$$I=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\ a=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix},\ b=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

是对称群S_3:

$$I=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix},\ a=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix},\ b=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},$$
$$c=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},\ d=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix},\ e=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

的不变子群. 这是可以具体加以验证的. 例如，用S_3中的元素$c=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$将$A_3$中的元素$a=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$加以变形，得

$$c^{-1}cc=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}^{-1}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=b,$$

仍为 A_3 中的元素．类似地有 $d^{-1}ad=b$, $e^{-1}ae=b$, $c^{-1}bc=a$, $d^{-1}bd=a$, $e^{-1}be=a$. 读者可以自己进行具体计算加以验证．由此可见，用 S_3 中任一元素将 A_3 中任一元素加以变形，所得仍为 A_3 中的一个元素，故 A_3 是 S_3 的一个不变子群．

G 本身及 I 当然也是 G 的不变子群，这两个子群称为 G 的平凡不变子群．

我们再来看一个例子．

[例 2]　子群 H:

$$I=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad a=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

是群 A_4:

$$I=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad a=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$

$$b=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\quad c=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},$$

$$d=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\quad e=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},$$

$$f=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\quad g=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},$$

$$h=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\quad i=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},$$

$$j=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\quad k=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$$

的子群，但是因为

$$\begin{aligned}d^{-1}ad&=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}^{-1}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\\&=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\\&=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\end{aligned}$$

这已不再是 H 的元素了，所以 H 不是 A_4 的不变子群.

极大不变子群 若 H 是 G 的不变子群，且 G 中没有包含 H 的非平凡不变子群，则称 H 是 G 的极大不变子群.

容易证明交代群 A_n 必为对称群 S_n 之极大不变子群. 这是因为，若 g 是一偶置换(即 g 属于 A_n)，h 为G中一任意置换，则$h^{-1}gh$ 仍是偶置换(即 $h^{-1}gh$ 仍属于 A_n). 所以 A_n 是 S_n 的一个不变子群. 而

$$\frac{S_n\text{的阶数}}{A_n\text{的阶数}}=\frac{n!}{\frac{n!}{2}}=2,$$

所以 A_n 是 S_n 的极大不变子群(为什么？请读者想一想).

合成群列 设 G 是一个群，H 是 G 的一个极大不变子群，而 K 又是 H 的一个极大不变子群，……，如此得到一列群:

$$G,\ H,\ K,\ \cdots,\ I.$$

列中每一个群必为其前一个群的极大不变子群，而列中最后一个群 I 必定是仅由恒等元构成的. 这一列群称为 G 的**合成群列**.

组合因数 设群 G 的合成群列 $G, H, K, \cdots, I$ 的阶数分别为 $n, n_1, n_2, \cdots, 1$ 则称正整数列 $\frac{n}{n_1}, \frac{n_1}{n_2}, \frac{n_2}{n_3}, \cdots$ 为群 G 的组合因数.

可解群 组合因数都是素数的群称为可解群.

下面我们可以看到，每一代数方程均有一群，当且仅当此方程的群是可解群时，此方程才可用代数方法求解．具体地说，我们在下一章里将证明：首项系数为 1，其他项系数为文字的一般 n 次方程所对应的群（称为它的伽罗华群），就是 n 个文字的所有置换（共 $n!$ 个）所构成的对称群 S_n．因此一般的 n 次方程是否可解的关键在于对称群 S_n 是否是可解群（也就是 S_n 的组合因数是否都是素数）？

下面我们要来证明：

定理 *当 $n>4$ 时，对称群 S_n 均不可解.*

有了这一定理，立刻就可证明高于四次的一般代数方程不可能用代数方法求解.

我们已经知道交代群 A_n 是对称群 S_n 的极大不变子群，下面再来证明当 $n>4$ 时交代群 A_n 除了 I（仅由恒等置换所构成的子群）外，并无其它不变子群．如果能证明这一点，S_n，A_n，I 就构成了对称群 S_n 的合成群列．相应的组合因素为

$$\frac{n!}{\frac{n!}{2}}=2, \quad \frac{\frac{n!}{2}}{1}=\frac{n!}{2}.$$

当 $n>4$ 时 $\frac{n!}{2}$ 显然不是素数，所以 S_n 也就不是可解群了.

为了证明 A_n 中除恒等置换 I 外并无其它不变子群，我们先引进一种表示置换的简单记法。

考察下面一些置换:

$$a=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\quad b=\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix},\quad c=\begin{pmatrix}1 & 2 & 4 & 3\\ 2 & 4 & 3 & 1\end{pmatrix},\cdots,$$

这些置换中有这样的特殊性质，上面一行中第一文字恰以第二文字代之，第二文字恰以第三文字代之，如此继续，直至最后一个文字用第一文字代之. 这种特殊形式的置换称为轮换. 对于轮换可用简单记号记之如下:

$$a=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=(1\quad 2\quad 3),$$

$$b=\begin{pmatrix}1 & 3 & 2\\ 3 & 2 & 1\end{pmatrix}=(1\quad 3\quad 2),$$

$$c=\begin{pmatrix}1 & 2 & 4 & 3\\ 2 & 4 & 3 & 1\end{pmatrix}=(1\quad 2\quad 4\quad 3)$$

显然在上述记号中，将轮换中各文字作一轮换排列，其结果不变，就是说:

$$a=(1\quad 2\quad 3)=(2\quad 3\quad 1)=(3\quad 1\quad 2),$$

$$b=(1\quad 3\quad 2)=(3\quad 2\quad 1)=(2\quad 1\quad 3),$$

$$c=(1\quad 2\quad 4\quad 3)=(2\quad 4\quad 3\quad 1)=(4\quad 3\quad 1\quad 2)$$
$$=(3\quad 1\quad 2\quad 4),\cdots.$$

容易看出: 任何一个置换均可表成含不同文字的轮换的乘积，如

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}=(1\quad 2)(3\quad 4),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 3 & 2\end{pmatrix}=(1\quad 4\quad 2)(3)=(1\quad 4\quad 2).$$

仅含一文字的置换显然可略去不写，不会引起混淆.

$$\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix}=(2\quad 4\quad 3\quad 5).$$

此外还容易看出：若 a 是 k 个文字的轮换，则 $a^k=I$ 为恒等置换.

仅有两文字的轮换

$$(\alpha_1\quad\alpha_2)=\begin{pmatrix}\alpha_1&\alpha_2\\\alpha_2&\alpha_1\end{pmatrix},$$

称为对换．显然任一轮换均可表为对换的乘积：

$$(\alpha_1\alpha_2\cdots\alpha_k)=(\alpha_1\alpha_2)(\alpha_1\alpha_3)\cdots(\alpha_1\alpha_k),$$

因此任一置换均可化成对换的乘积．因为每一对换使函数

$$\phi(x_1,\ x_2,\ \cdots,\ x_n)=(x_1-x_2)(x_1-x_3)\cdots(x_2-x_3)$$
$$\cdots(x_2-x_n)\cdots(x_{n-1}-x_n).$$

改变符号，即

$$(\alpha_1\alpha_2):\ \phi(x_1,\ \cdots,\ x_n)\Rightarrow-\phi(x_1,\ \cdots,\ x_n).$$

所以偶置换应该是化为偶数个对换的乘积，而奇置换则化为奇数个置换的乘积.

现在用反证法来证明，当 $n>4$ 时，A_n 除 I 外无其它不变子群：

如果 A_n 除 I 外尚有不变子群 $H\neq I$，则 H 必含有 I 以外的置换．将这些置换都表成不同文字的轮换的乘积．现设 h 为 H 中所变文字为最少的一个置换，则

(i) 将 h 表示为轮换的乘积形式中各轮换必含相同个数的文字，因为，否则若

$$h=(\alpha_1\alpha_2\cdots\alpha_k)(\beta_1\beta_2\cdots\beta_k\beta_{k+1}\cdots)\cdots,$$

则 k 个 h 的乘积 $hh\cdots h=h^k$ 必然不改变 $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_k$（因为 $(\alpha_1\alpha_2\cdots\alpha_k)^k=I$）而又不会使 h 中增加原来没有的文字，而 h^k 也是一个置换，它所变之文字比 h 所变的文字要少（少 $\alpha_1,\ \alpha_2,$

$\cdots, a_k)$，这与 h 的所变文字为最少这一假设矛盾.

(ii) h 的乘积中的各个轮换不能含有三个以上的文字，这是因为，如果乘积中有一个轮换含有四个或四个以上文字，比如说：

$$h=(1\ 2\ 3\ 4\cdots)(\cdots)\cdots,$$

则用 A_n 中之偶置换 $g=(2\ 3\ 4)$ 将 h 变形，得：

$$h_1=g^{-1}hg=(2\ 4\ 3)(1\ 2\ 3\ 4\cdots)(\cdots)\cdots(2\ 3\ 4)$$
$$=(1\ 3\ 4\ 2\cdots)(\cdots),$$

这里以…省略的文字与原来 h 中相同. 因 H 是 A_n 之不变子群，所以 h, h_1 及 hh_1^{-1} 仍属于 H. 但

$$hh_1^{-1}=(2\ 3\ 4),$$

于是 hh_1^{-1} 所变的文字少于 h 所变之文字. 这又与 h 的定义矛盾.

(iii) h 只能是一个轮换，而不能是 n 个轮换之乘积. 这是因为：

(a) 如 $h=(1\ 2)(3\ 4)$，因 $n>4$ 故可取 A_n 中的偶置换 $g=(1\ 2\ 5)$，使

$$hg^{-1}hg=(1\ 2)(3\ 4)(2\ 1\ 5)(1\ 2)(3\ 4)(1\ 2\ 5)$$
$$=\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}3&4\\4&3\end{pmatrix}\begin{pmatrix}2&1&5\\1&5&2\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}3&4\\4&3\end{pmatrix}\begin{pmatrix}1&2&5\\2&5&1\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix}=(1\ 5\ 2).$$

于是 $hg^{-1}hg$ 属于 H，而它所变的文字少于 h 所变的文字. 又与 h 之定义矛盾.

(b) 如 $h=(1\ 2\ 3)(4\ 5\ 6)\cdots$，可仍取 $g=(1\ 2\ 5)$，则

$$h^{-1}g^{-1}hg=(1\ 2\ 6\ 3\ 5).$$

它所变的文字亦少于 h 所变的文字．也导致矛盾．

总结以上讨论可知，若 h 为 H 中所变文字最少者，则 h 的形式只可能是：

$$h=(\alpha_1\alpha_2) \quad 或 \quad h=(\alpha_1\alpha_2\alpha_3),$$

但 h 属于 H，而 H 又是 A_n 之子群，所以 h 必为偶置换，因而 h 不可能等于 $(\alpha_1\alpha_2)$，故 h 必为 $(\alpha_1\alpha_2\alpha_3)$ 形式．而任意三文字的轮换 $(\beta_1\beta_2\beta_3)$ 均可由 $(\alpha_1\alpha_2\alpha_3)$ 用偶置换

$$g=\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3\\ \beta_1 & \beta_2 & \beta_3\end{pmatrix}$$

变形而得：

$$\begin{pmatrix}\beta_1 & \beta_2 & \beta_3\\ \alpha_1 & \alpha_2 & \alpha_3\end{pmatrix}(\alpha_1\ \alpha_2\ \alpha_3)\begin{pmatrix}\alpha_1 & \alpha_2 & \alpha_3\\ \beta_1 & \beta_2 & \beta_3\end{pmatrix}=(\beta_1\ \beta_2\ \beta_3),$$

$(\beta_1\beta_2\beta_3)$ 当然在 H 中，所以 H 含有一切三文字的轮换．因为 A_n 中之置换均为偶置换，故可表为偶数个对换的乘积，即若 g 属于 A_n，则 $g=t_1t_2t_3t_4\cdots t_{2k-1}t_{2k}$．其中 $t_1, t_2, \cdots, t_{2k}$ 是对换．若

(i) $t_1=t_2$，则 $t_1t_2=I$；

(ii) t_1 与 t_2 有一文字相同，则

$$t_1t_2=(\alpha\beta)(\alpha\gamma)=(\alpha\beta\gamma),$$

(iii) t_1 与 t_2 无相同文字，则

$$\begin{aligned}t_1t_2=(\alpha\beta)(\gamma\delta)&=(\alpha\beta)(\alpha\gamma)(\gamma\alpha)(\gamma\delta)\\&=(\alpha\beta\gamma)(\gamma\alpha\delta).\end{aligned}$$

对 $t_3t_4\cdots t_{2k-1}t_{2k}$ 可完全类似地讨论，所以任一偶置换均可表成三文字的轮换的乘积．也就是说 A_n 中的元素都在 H 中，但 H 又是 A_n 的子群，因此 H 必定就是 A_n，这就证明了 A_n 除 I 外不含其它非平凡不变子群．

四、数域与代数式的可约性. 代数方程的伽罗华群

1. 数域与代数多项式的可约性

学过中学代数的人对于因式分解都是很熟悉的，例如

$$x^2-4=(x+2)(x-2),$$

$$x^2+3x+2=(x+1)(x+2),$$

等等. 我们所要讨论的解代数方程的问题与完全分解成一次因式有着密切的联系. 例如，给定了方程

$$x^2+x-2=0,$$

如我们能将 x^2+x-2 分解成 $(x-1)(x+2)$ 就等于求得此方程的解 $x=1$ 与 $x=-2$. 反之，如求得了方程

$$x^2+3x+2=0$$

的两个根 $x=-1$, $x=-2$, 就可将 x^2+3x+2 分解为 $(x+1)(x+2)$.

一般地说，给定一个代数方程

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0, \tag{4.1}$$

若我们能将相应的多项式

$$p_n(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

分解成一次因子的乘积：

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=(x-x_1)(x-x_2)\cdots(x-x_n), \tag{4.2}$$

那就等于求得了方程(5.1)的全部根 $x_1, x_2, \cdots, x_n$. 反之，若已求得方程(5.1)的 n 个根 $x_1, x_2, \cdots, x_n$, 那么首项系数为1

的多项式 $p_n(x)$ 就可进行因式分解：

$$p_n(x)=(x-x_1)(x-x_2)\cdots(x-x_n).$$

但必须着重指出的是，一个多项式能不能进行因式分解，与我们所讨论的数的范围有着密切关系．例如，在没有引入复数以前，x^2+1 是不能再分解因式了．而在引入了复数以后，x^2+1 就可以分解成 $(x-i)(x+i)$．同样，要是限制在有理数的范围内 x^2-2 就不可能再分解了．但在无理数范围内 x^2-2 却可分解成 $(x-\sqrt{2})(x+\sqrt{2})$．由此可见，我们要讨论一个多项式的因式分解问题，必须先讲清楚系数是限制在什么范围内．为了说清系数限制的范围，我们引入数域的概念．

一个至少包含两个数的集合（可以是实数，也可以是复数），如果其中任意两数作加、减、乘、除（但不用 0 为除数）所得之结果仍在此集合内，则称这个数的集合为一数域，简称为域．以后常用 F，K，…大写字母记数域；而用小写字母 q，r，s，…记数域中的数．

［例 1］　一切实数所组成的集合是一数域，记作 $\mathbf{R}$，这个数域称为实数域．

［例 2］　一切复数所组成的集合是一数域，记作 $\mathbf{C}$，这个数域称为复数域．

［例 3］　一切有理数所组成的集合是一数域，记作 $\mathbf{Q}$，这个数域称为有理数域．

以上三例都是显然的，读者可以自行验证．

［例 4］　一切 $a+b\sqrt{2}$ 形式的实数（这里 a，b 可取任意有理数）所组成的集合成一数域，这个数域今后记为 $\mathbf{Q}(\sqrt{2})$，它是包含 $\mathbf{Q}$ 与 $\sqrt{2}$ 的最小数域．我们来验证 $\mathbf{Q}(\sqrt{2})$ 确为一个数域．事实上若 $a_1+b_1\sqrt{2}$ 与 $a_2+b_2\sqrt{2}$ 是 $\mathbf{Q}(\sqrt{2})$

中的两个数，则

$$(a_1+b_1\sqrt{2})\pm(a_2+b_2\sqrt{2})=(a_1\pm a_2)+(b_1\pm b_2)\sqrt{2},$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})$$
$$=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$$

都仍是 $\mathbf{Q}(\sqrt{2})$ 中的数．且当 $a_2+b_2\sqrt{2}\neq0$ 即 $a_2^2+b_2^2\neq0$ 时

$$\frac{a_1+b_1\sqrt{2}}{a_2+b_2\sqrt{2}}=\frac{(a_1+b_1\sqrt{2})(a_2-b_2\sqrt{2})}{(a_2+b_2\sqrt{2})(a_2-b_2\sqrt{2})}$$
$$=\frac{a_1a_2-2b_1b_2}{a_2^2-2b_2^2}+\frac{a_2b_1-a_1b_2}{a_2^2-2b_2^2}\sqrt{2}$$

也是 $\mathbf{Q}(\sqrt{2})$ 中的数（因为 a_2, b_2 均为非零有理数，所以 $a_2^2-2b_2^2\neq0$）．根据数域的定义，$\mathbf{Q}(\sqrt{2})$ 确是数域．

关于 $\mathbf{Q}(\sqrt{2})$ 是包含 $\mathbf{Q}$ 与 $\sqrt{2}$ 的最小数域，只要证明任何包含 $\mathbf{Q}$ 与 $\sqrt{2}$ 的域都包含 $\mathbf{Q}(\sqrt{2})$ 在内，这一点留给读者证明．

[例 5]　一切 $a+bi$ 形式的复数（这里 a, b 为任意有理数）所组成的集合是一数域，此数域今后记为 $\mathbf{Q}(i)$，它是包含 i 的最小数域．读者可以自行验证．

[例 6]　一切整数所成之集合不是数域，这是因为两个整数之商未必仍是整数．

[例 7]　一切正数所成之集合不是数域，这是因为两个正数之差未必仍是正数．

我们把包含数 a_1, a_2, …, a_n 的最小的数域，叫做由 a_1, …, a_n 生成的数域．根据数域的定义，由 a_1, …, a_n 生成的数域就是由这些数任意地经过加、减、乘、除而得到的所有结果（这些结果还可以反复地参加上述运算）组成的．

凡是数域都包含 0 与 1 这两个数．这是因为根据数域的

定义，在数域中任取一数 $a\neq 0$，则 $a-a=0$，$\frac{a}{a}=1$ 必属于此数域．但是由 1 就可以生成有理数域 $\mathbf{Q}$（为什么？），由此即知任意数域必含有全体有理数（为什么？）．

实域　若一域中的数均为实数，则称此域为实域．注意实域与实数域不是一回事，实数域包含所有的实数．

可约与不可约　若系数属于数域 K 的多项式 $P(x)$ 可表成两个系数亦属于 K 且次数 $\geqslant 1$ 次的多项式的乘积，则称此多项式在 K 上可约，否则称为在 K 上不可约．由不可约多项式 $P(x)$ 所构成的方程就称为不可约的方程（当然必须指明在什么域上）．

［例 8］　多项式 x^2-2 在有理数域 $\mathbf{Q}$ 上不可约，但在实数域 $\mathbf{R}$ 上可约．在数域 $\mathbf{Q}(\sqrt{2})$ 上也可约．所以 $x^2-2=0$ 是域 $\mathbf{Q}$ 上的不可约方程，但它是域 $\mathbf{Q}(\sqrt{2})$ 或 $\mathbf{R}$ 上的可约方程．

［例 9］　多项式 x^2+1 在实数域 $\mathbf{R}$ 上不可约，但在复数域 $\mathbf{C}$ 上可约．所以 $x^2+1=0$ 是域 $\mathbf{R}$ 上的不可约方程，但它是域 $\mathbf{C}$ 上的可约方程．

今后，如果多项式 $f(x)$ 的系数取在域 K 中，我们就称 $f(x)$ 是域 K 上的多项式，$f(x)=0$ 就称为是域 K 上的方程．

2. 域的扩张．扩张的维数

从上一节的最后两个例子可见，一个数域 F 上的多项式，可能在 F 中不可约．系数在 F 上的多项式，未必能分解成系数在 F 中的非常数多项式的乘积．但是将数域 F 扩大后，就有可能变成可约的了．如 x^2-2 在有理数域 $\mathbf{Q}$ 上不可约，但是将 $\mathbf{Q}$ 扩大为实数域 $\mathbf{R}$ 后，它就是可约的了．又如

x^2+1 在实数域 $\mathbf{R}$ 上不可约，但将 $\mathbf{R}$ 扩大为复数域 C 后，它就是可约的了.

为此我们引进域的扩张的概念：

若数域 F 的数都属于数域 K，则称 K 为 F 的扩张域. 简称 K 是 F 的扩域. 同时称 F 是 K 的子数域，简称为 F 是 K 的子域. 记为 $F\subset K$.

若三个数域：F，M，K 满足 $F\subset M\subset K$，则称 M 是 F 与 K 的中间域.

［例 1］ 实数域 $\mathbf{R}$ 是有理数域 $\mathbf{Q}$ 的扩域，同时有理数域 $\mathbf{Q}$ 是实数域 $\mathbf{R}$ 的子域，即 $\mathbf{Q}\subset\mathbf{R}$. 前面说明过：任意数域必包含有理数域 $\mathbf{Q}$，因而任何数域都是 $\mathbf{Q}$ 的扩域，$\mathbf{Q}$ 是任何数域的子域.

［例 2］ 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的扩域，即 $R\subset C$.

［例 3］ 域 $Q(\sqrt{2})$ 是有理数域 $\mathbf{Q}$ 的扩域，而实数域 $\mathbf{R}$ 又是域 $\mathbf{Q}(\sqrt{2})$ 的扩域，这就是说域 $\mathbf{Q}(\sqrt{2})$ 是有理数域 $\mathbf{Q}$ 与实数域 $\mathbf{R}$ 的中间域，即 $\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})\subset\mathbf{R}$.

由第一节的讨论中可见域的扩张与多项式的因式分解有密切联系，因而与代数方程的求解有密切的联系. 对于本书说来最重要的扩张方法是将一个代数方程的根添加到一个数域中去所生成的扩张. 这就是所谓代数扩张. 下面我们就来仔细讨论一下与代数扩张有关的问题.

前面我们已看到域 $Q(\sqrt{2})$ 是域 $\mathbf{Q}$ 的扩张. 这种扩张可看成在数域 $\mathbf{Q}$ 上添加 $\sqrt{2}$（即方程 $x^2-2=0$ 的一个根），再用加、减、乘、除生成的一个域. 注意，光把 $\mathbf{Q}$ 添上 $\sqrt{2}$ 一个元素并不构成域. $Q\sqrt{2}$ 的具体内容是所有 $a+b\sqrt{2}$ 形式的数，这里 a、b 属于 $\mathbf{Q}$. 前面说过，容易证明 $\mathbf{Q}(\sqrt{2})$ 也是 $\mathbf{Q}$ 的包含 $\sqrt{2}$ 的扩域中之最小者. 我们称域 $\mathbf{Q}(\sqrt{2})$ 是由 $\mathbf{Q}$ 添

加$\sqrt{2}$所生成的$\mathbf{Q}$的扩域. 前面例子中的$Q(i)$也与此类似，是$\mathbf{Q}$添加i生成的$\mathbf{Q}$的扩域，它也是$\mathbf{Q}$的含i的扩域之最小者，其具体内容是所有形如$a+bi$的数，这里a、b属于$\mathbf{Q}$.

一般说来，设c是一个数域F上的不可约代数方程

$$h_0+h_1x+\cdots+h_{n-1}x^{n-1}+h_nx_n=0$$

的根(这里h_0, h_1, $\cdots$, h_n属于F)，那么可以证明所有

$$a_0+a_1c+a_2c^2+\cdots+a_{n-1}c^{n-1}$$

形式的数(这里a_0, a_1, $\cdots$, a_n可以在F中任取)必定构成一个数域，我们把它记为$F(c)$. 而且这个域$F(c)$是F的包含c的扩域中之最小者，我们称$F(c)$是由F添加数c所生成的. 这种扩域称为代数扩域.

从上面的定义知，$F(c)$中的数都可表成

$$a_0+a_1c+a_2c^2+\cdots+a_{n-1}c^n,$$

而且可以证明这表示方法是唯一的. 这一组数1、c、c^2、$\cdots$、c^{n-1}的个数n就称为扩域$F(c)$相对于域F的维数，并把维数n记为

$$n=[F(c):F].$$

这时也称域$F(c)$是F的n次扩域.

[例 4] 域$\mathbf{Q}(\sqrt{2})$是由$\mathbf{Q}$添加$\sqrt{2}$而生成的，而$\sqrt{2}$是$\mathbf{Q}$上不可约方程$x^2-2=0$的根. 所以$\mathbf{Q}(\sqrt{2})$相对于$\mathbf{Q}$的维数是2, 即$2=[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]$. $\mathbf{Q}(\sqrt{2})$中的任何数都可以写成$a+b\sqrt{2}$(a、b属于$\mathbf{Q}$)的形式.

这种由一个数域F添加F上的一个不可约代数方程的根c而生成扩域$F(c)$的方法，可以重复进行多次：我们可再取域$F(c)$上一个不可约代数方程的根c_1，将c_1添加到域$F(c)$上生成$F(c)(c_1)$，这可简记为$F(c, c_1)$. 而且这是F的包含c、c_1的扩域中之最小者.

[例5] 将 $\mathbf{Q}$ 上不可约方程 $x^2-2=0$ 的根 $\sqrt{2}$ 添加于 $\mathbf{Q}$ 生成域 $\mathbf{Q}(\sqrt{2})$，再将 $Q(\sqrt{2})$ 上不可约方程 $x^2+1=0$ 的根 $i=\sqrt{-1}$ 添加于 $Q(\sqrt{2})$ 生成域 $Q(\sqrt{2}, i)$，它是由一切

$$a+b\sqrt{2}+ci+di\sqrt{2}$$

形式的数(a、b、c、d 属于 Q)所构成的.

将 $\mathbf{Q}$ 上不可约方程 $x^4-2x^2+9=0$ 的一个根 $i+\sqrt{2}$ 添加于 $\mathbf{Q}$ 而生成扩域 $\mathbf{Q}(i+\sqrt{2})$. 它是由所有

$$\alpha+\beta(i+\sqrt{2})+\gamma(i+\sqrt{2})^2+\delta(i+\sqrt{2})^3$$

形式的数所组成的(α、β、γ、δ 属于 $\mathbf{Q}$)，化简以后，也就是由一切

$$(\alpha+\gamma)+(\beta-\delta)\sqrt{2}+(\beta+5\delta)i+2\gamma\sqrt{2}i$$

形式的数所构成的. 不难看出，由 a、b、c、d 可以唯一确定 α、β、γ、δ，反之亦然. 可见域 $\mathbf{Q}(\sqrt{2}, i)$ 与 $\mathbf{Q}(\sqrt{2}+i)$ 是相同的，而且显然与域 $\mathbf{Q}(i, \sqrt{2})$ 也是相同的. 我们注意到，

$$\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})\subset\mathbf{Q}(\sqrt{2}, i),$$

$$[Q(\sqrt{2}):Q]=2,\ [Q(\sqrt{2}, i):Q(\sqrt{2})]=2,$$

$$[Q(\sqrt{2}+i):Q]=[Q(\sqrt{2}, i):Q]=[Q(i, \sqrt{2}):Q]=4.$$

从 $$4=2\times 2,$$

即有

$$[Q(i, \sqrt{2}):Q]=[Q(i, \sqrt{2}):Q(\sqrt{2})]\ [Q(\sqrt{2}):Q].$$

上面虽然仅是一个对特殊情况进行计算得到的结果，但它却启示着一个普遍的规律，一般地我们有下面的

定理1 设 c_1 是域 F 上的不可约代数方程的根，c_2 是域 $F(c_1)$ 上不可约代数方程的根，则将 c_2 添加于 $F(c_1)$ 所生成的扩域 $F(c_1, c_2)$，与将 c_1 添加于 $F(c_2)$ 所生成的扩域 $F(c_2, c_1)$ 是相同的，而且存在 F 上一个不可约代数方程的根 c，使

$$F(c)=F(c_1, c_2)=F(c_2, c_1).$$

定理2 若域 K 是域 F 的代数扩域，域 L 是域 K 的代数扩域：$F\subset K\subset L$，则

$$[L:F]=[L:K][K:F].$$

这两个定理证明从略. 由定理2容易得到简单有用的系：

系 若域 K 是域 F 的代数扩域，且 $n=[K:F]$，u 为 K 中任意一数. 则 $[F(u):F]$ 必能整除 n.

证明 这是因为 $F(u)$ 是 K 与 F 的中间域：$F\subset F(u)\subset K$，所以

$$n=[K:F]=[K:F(u)][F(u):F].$$

因 $[K, F(u)]$ 必为正整数，所以 $[F(u):F]$ 必能整除 n.

我们特别引进一个定义，当 $[K:F]$ 是一个有限的数目时，称 K 是 F 的有限扩域.

上面的定理可以推广到更一般的情况：在域 F 上逐次添加代数方程的根 $c_1, c_2, c_3, \cdots, c_k$，得到的扩域 $F(c_1, c_2, \cdots, c_k)$ 是与添加的次序无关的，而且存在 F 上的一个不可约代数方程的根 c，使

$$F(c)=F(c_1, c_2, \cdots, c_k).$$

3. 代数方程的根域. 正规域

根域 从一些具体例子我们看出，对数域 F 上某些 n 次代数方程 $f(x)=0$，只要将数域 F 加以适当扩张，必可使 $f(x)$ 在这个扩域上分解为一次因子的乘积. 事实上，这对任何代数方程都是成立的. 令 $f(x)=0$ 在某个很大的域里有 n 个根 $u_1, u_2, \cdots, u_n$，逐次将 $u_1, u_2, \cdots, u_n$ 添加到 F 上所生成的扩张域记为 $F(u_1, u_2, \cdots, u_n)$（由上节的定理1知这个

扩张域与 $u_1, u_2, \cdots, u_n$ 的排列次序无关)，则 $f(x)$ 在 $F(u_1, u_2, \cdots, u_n)$ 显然可以分解为一次因子的乘积：

$$f(x)=(x-u_1)(x-u_2)\cdots(x-u_n),$$

而且 $F(u_1, u_2, \cdots, u_n)$ 是使 $f(x)$ 能分解成一次因子乘积的扩张域中之最小者．我们称这个域 $F(u_1, u_2, \cdots, u_n)$ 为方程 $f(x)=0$ 的根域．而且由上节定理 1 知，F 上一定存在一个数 c 使

$$F(u_1, u_2, \cdots, u_n)=F(c),$$

并且 c 是 F 上某个不可约方程的根．

例如，有理数域 $\mathbf{Q}$ 上的方程 $x^3-5=0$ 它有三个根

$$\sqrt[3]{5},\ \omega\sqrt[3]{5},\ \omega^2\sqrt[3]{5},$$

因此它的根域为 $\mathbf{Q}(\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5})$，事实上这个数域可由 $\mathbf{Q}$ 添加 $\sqrt[3]{5}$ 与 ω 这两个数而生成，即 $\mathbf{Q}(\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5})=\mathbf{Q}(\sqrt[3]{5}, \omega)$，显然 $[\mathbf{Q}(\sqrt[3]{5}):\mathbf{Q}]=3$．而 ω 在数域 $\mathbf{Q}(\sqrt[3]{5})$ 上满足不可约方程 $x^2+x+1=0$，所以 $[\mathbf{Q}(\sqrt[3]{5}, \omega):\mathbf{Q}(\sqrt[3]{5})]=2$．因此由上节定理 2 知

$$\begin{aligned}[\mathbf{Q}(\sqrt[3]{5}, \omega):\mathbf{Q}]&=[\mathbf{Q}(\sqrt[3]{5}, \omega):\mathbf{Q}(\sqrt[3]{5})]\cdot[\mathbf{Q}(\sqrt[3]{5}):\mathbf{Q}]\\&=2\times3=6.\end{aligned}$$

域 F 上的共轭数　我们称复数 $a+bi$ 与 $a-bi$ 是相互共轭的，它们满足实数域 $\mathbf{R}$ 上的一个不可约方程(设 $b\neq0$)：

$$[x-(a+bi)][x-(a-bi)]=0,$$

即

$$x^2-2ax+(a^2+b^2)=0.$$

现在我们将上述共轭的概念加以推广．我们说 $\sqrt{2}$ 与 $-\sqrt{2}$ 是在有理数域 $\mathbf{Q}$ 上是共轭的，因为它们满足一个在有理数域 $\mathbf{Q}$ 上不可约的方程 $x^2-2=0$．一般地，对数域 K 中两个数 u, v，若它们满足 K 的子域 F 上的同一个不可约方程，则我

们称 u, v 在数域 F 上是共轭的.

例如, $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$ 与 $\omega^2\sqrt[3]{5}$ 都满足有理数域 $\mathbf{Q}$ 上的不可约方程 $x^3-5=0$, 所以我们说 $\sqrt[3]{5}$, $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$ 这三个数在有理数域 $\mathbf{Q}$ 上是共轭的.

因 $\mathbf{Q}(\sqrt[3]{5})$ 是一个实域, 所以 $Q(\sqrt[3]{5})$ 肯定不会包含 $\omega\sqrt[3]{5}$, $\omega^2\sqrt[3]{5}$. 所以一般说来, 如果 u 是 F 的扩域 K 中的一个数, u^* 是 u 在 F 上的一个共轭数, 即 u 与 u^* 共同满足 F 上的一个不可约方程, 则 u^* 不一定属于 K. 上面指出的 $\mathbf{Q}(\sqrt[3]{5})$ 就是这种扩域. 但是有一类特殊的扩域, 它若含有 u, 则必含有其所有的共轭数, 这就是正规扩域.

正规扩域 设 N 是 F 的扩域, 如果 u 属于 N, 且 u 在 F 上的共轭数也属于 N, 这样的扩域 N 称为 F 的**正规扩域**.

关于正规扩域我们有下面重要的定理:

定理 域 F 的有限扩域 N 是正规扩域的充要条件 N 是 F 上某一方程的根域.

我们仅证必要性, 充分性的证明较复杂, 就略去了.

证 必要性: 设 N 是 F 的正规扩张域, 在 N 中任取一不属于 F 的数 u. 设 $p(x)$ 为 u 所满足的 F 上不可约方程, 则由正规扩域的定义知 N 包含 $p(x)=0$ 的一切根, 所以 N 必包含 $p(x)=0$ 的根域 M. 若在 N 中尚有不属于 M 的数, 取其中一个记为 v, 设 v 满足 F 上不可约方程 $q(x)=0$, 则 M 必含在 $p(x)q(x)=0$ 的根域 L 中, 而且由于 N 是正规扩张, 所以 L 必含在 N 中. 这样我们就得到 M, L, $\cdots$, 这一系列根域, 而且

$$F\subset M\subset L\subset\cdots\subset N$$

因为 N 是 F 的有限扩域, 所以这样逐次扩大根域不能进行无限次(否则由上节定理 2 把维数相乘将引出矛盾), 而只要

扩大的根域不等于 N 就还可以扩大. 这两方面综合起来，就知道进行有限次扩张后，扩大的根域必然等于 N. 这就是说，N 是 F 上某一方程的根域.

4. 数域的自同构群

在本书的二、三章中大家已经看到了置换群在一般代数方程求解问题中所起的作用. 特别重要的是在 29 页中所引进的拉格朗日的两个命题. 伽罗华发展了拉格朗日的理论. 伽罗华的理论不仅可以解决一般文字系数的代数方程的代数求解公式是否存在的问题，而且可以解决具体数字系数方程的求解问题. 为此，我们要将根的置换群的理论稍加推广，研究数域的自同构群.

我们先来考察一个方程 $x^4-10x^2+1=0$, 它有 4 个根：

$$x_1=\sqrt{2}+\sqrt{3}, \quad x_2=\sqrt{2}-\sqrt{3},$$
$$x_3=-\sqrt{2}+\sqrt{3}, x_4=-\sqrt{2}-\sqrt{3}.$$

可见为了求得这个方程的 4 个根，除了对方程的系数作加、减、乘、除等有理运算外，还必须作两次开方运算以得到 $\sqrt{2}$ 与 $\sqrt{3}$.

方程 $x^4-10x^2+1=0$ 的系数 -10, 1 生成的数域即有理数域 $\mathbf{Q}$. 在这个数域中 $x^4-10x^2-1=0$ 是不可约的. 而当我们将 $\sqrt{2}$ 添加到有理数域 $\mathbf{Q}$ 中将它扩大为数域 $\mathbf{Q}(\sqrt{2})$ 后，方程 $x^4-10x^2+1=0$ 就可以分解成

$$(x^2-2\sqrt{2}x+1)(x^2+2\sqrt{2}x+1)=0.$$

但上面方程中的两个因子在数域 $\mathbf{Q}(\sqrt{2})$ 中是不能再分解了. 要是我们再将 $\sqrt{3}$ 添加到数域 $\mathbf{Q}(\sqrt{2})$ 中去将它进一步扩大为 $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ (这个数域是由所有形为 $a+b\sqrt{2}$

$+c\sqrt{3}+d\sqrt{6}$的数所构成的，这里a，b，c，d是任意有理数)，那么上面方程又可进一步分解成一次因子的乘积：

$$[x-(\sqrt{2}+\sqrt{3})][x-(\sqrt{2}-\sqrt{3})]$$
$$\times[x-(-\sqrt{2}+\sqrt{3})][x-(-\sqrt{2}-\sqrt{3})]=0$$

这样就等于求得了方程$x^4-10x^2+1=0$的4个根.

所以用加、减、乘、除与开方来求解代数方程的过程，实质上就是从方程的系数域出发，逐次添加适当的根式来扩大数域，使得原来不能分解的方程逐步分解，以致最后能分解成全部是一次因式的乘积.

一般地说，设方程

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n=0$$

的系数生成的域为F，N是它的根域(也就是说此方程在数域N上可以分解成一次因子的乘积，从而可解)，这个方程是否可用代数方法求解的关键问题是：数域F是否可以经过有限次添加根式而扩张为根域N，也就是说是否存在有限多个中间域F_1，F_2，$\cdots$，F_{s-1}，F_s使

$$F\subset F_1\subset F_2\cdots\subset F_s=N,$$

并且其中每一个F_i都是由F_{i-1}添加F_{i-1}中的数的根式而成的扩域，而且由于

$$\sqrt[st]{a}=\sqrt[s]{\sqrt[t]{a}},$$

所以当根指数是复合数时，可以把这个根式的一次添加等价于连续添加几次，每次添加的根指数都是素数次根．也就是说：不妨设每次所添加的根式都是素数次根.

那么这样的中间域F_i与F_{i-1}之间应该有什么关系呢？经过伽罗华的研究，弄清楚了关键取决于：使F_{i-1}保持不变的F_i的自同构变换群的结构．为了使大家能更看清楚问题的本质，我们还是先来具体考察一下以前见过的简单例子.

域$\mathbf{Q}(\sqrt{2})$是由有理数域$\mathbf{Q}$添加$\mathbf{Q}$中的数2的根式$\sqrt{2}$而生成的. $\mathbf{Q}(\sqrt{2})$是$\mathbf{Q}$的二次扩域. 前面说过，域$\mathbf{Q}(\sqrt{2})$是由全体$a+b\sqrt{2}$形式的数所构成(其中a、b为任意有理数)，它是包含方程$x^2-2=0$的根($\sqrt{2}$与$-\sqrt{2}$)的最小数域，因而是$x^2-2=0$的根域. 我们来研究$\mathbf{Q}(\sqrt{2})$中数与$\mathbf{Q}$中的数之间的关系. 我们把$\mathbf{Q}(\sqrt{2})$的每一个数$a+b\sqrt{2}$换作$\mathbf{Q}(\sqrt{2})$中相应的另一个数$a-b\sqrt{2}$，这当然是一种变换，我们用S记这种变换，并用$(a+b\sqrt{2})S$记录$(a+b\sqrt{2})$用S作用后的结果，于是：

$$(a+b\sqrt{2})S=a-b\sqrt{2}.$$

而 $$[(a+b\sqrt{2})S]S=(a-b\sqrt{2})S=a+b\sqrt{2}.$$

这就是说将变换S连续施行两次的结果，等于不变换，或者说是恒等变换I. 类似于置换的乘积，变换也有乘法. 用乘法的记号，上述说法就是

$$S\cdot S=S^2=I.$$

所以I和S这两个变换就构成了一个变换群G(关于能构成群的原因下面还要讨论). 而且根据S的定义可见$\mathbf{Q}(\sqrt{2})$中属于$\mathbf{Q}$的那部分数在施行变换S时是不变的. 同时对$\mathbf{Q}(\sqrt{2})$中任意两数α, β有

$$(\alpha+\beta)S=\alpha S+\beta S,\ (\alpha\beta)S=\alpha S\cdot\beta S$$

(这就是所谓域的自同构，也放在下面详述). 这个群$G=\{I, S\}$称为域$\mathbf{Q}(\sqrt{2})$的能保持$\mathbf{Q}$不变的自同构变换群.

反之，如果有两域F与K，K是F的扩域：$F\subset K$，并且如果保持F不变的K的一切自同构变换群G仅由恒等变换I及另一变换T组成：$G=\{I, T\}$，那么必有$T\cdot T=I$. 并且这时K一定是F的二次扩域. 我们来证明这一点：对K中任一不属于F的数α，如果先用T作用得到结果设为α^*：

$\alpha T=\alpha^*$，则 α^* 再用 T 作用：

$$\alpha^*T=(\alpha T)T=\alpha I=\alpha.$$

且因 T 是自同构，据自同构的定义：

$$(\alpha+\alpha^*)T=\alpha T+\alpha^*T=\alpha^*+\alpha=\alpha+\alpha^*,$$

$$(\alpha\alpha^*)T=\alpha T\cdot\alpha^*T=\alpha^*\cdot\alpha=\alpha\alpha^*.$$

就是说，虽然 α, α^* 在 T 作用下未必不变，但 $\alpha+\alpha^*$ 与 $\alpha\cdot\alpha^*$ 在变换 T 作用下必定不变．根据 T 的定义，它们必定是 F 中的数，设为 l 与 m：

即 $$\alpha+\alpha^*=l,\quad \alpha\alpha^*=m.$$

所以 $$\alpha-\alpha^*=\sqrt{l^2-4m}.$$

$$\alpha=\frac{1}{2}l+\frac{1}{2}\sqrt{l^2-4m},$$

$$\alpha^*=\frac{1}{2}l-\frac{1}{2}\sqrt{l^2-4m}.$$

也就是说 α 必可表成 $a+b\sqrt{q}$ 的形式，这里 a, b, q 都是域 F 中的数．现在的 q 还是由 α 确定出来的，但我们可以进一步证明 K 中所有的数均可表成 $a+b\sqrt{q}$ 的形式，或者说域 K 是由域 F 添加 F 中确定的数 q 的平方根 $\sqrt{q}$ 所成的．由此可见 K 是 F 的二次扩张域．

综上所说，我们看到“K 是由 F 添加 F 中的数的平方根所生成”这件事，与“保持 F 中的数不变的 K 的自同构变换群仅由两个元素构成”是等价的．

上面讲的是最简单的特殊情况，但是它却揭示了伽罗华理论的根本原理，在一般情况下前面提到的 F_i 与 F_{i-1} 之间也有类似的关系，不过那时保持 F_{i-1} 不变的 F_i 的自同构变换群是一素数次的循环群，其次数正是 $[F_i:F_{i-1}]$．

因此为了说清伽罗华的理论，我们需要比较仔细地讨论

一下数域的自同构变换群，并给出比较严密的定义.

还是通过一个具体例子来说.

设 $\mathbf{C}$ 为复数域，我们将 $\mathbf{C}$ 中每一数 $a+bi$ 换成其共轭数 $a-bi$，用记号 T 表示这种变换:

$$(a+bi)T=a-bi,$$

这个变换 T 将 $\mathbf{C}$ 中的一个数一对一地变换为 $\mathbf{C}$ 中另一数.而且显然还满足

$$[(a_1+b_1i)+(a_2+b_2i)]T=(a_1+b_1i)T+(a_2+b_2i)T,$$

$$[(a_1+b_1i)\cdot(a_2+b_2i)]T=(a_1+b_1i)T\cdot(a_2+b_2i)T,$$

也就是将 $\mathbf{C}$ 中任意两个数先相加(或相乘)然后作变换，与先作变换后相加(或相乘)其结果是相同的.

一般说来，设 F 是任意一个数域. 如果变换 T 将 F 中的数一对一地变换成 F 中的数(即对任一 a 属于 F，aT 必属于 F，且当 $a\neq b$ 时 $aT\neq bT$)，同时满足:

$$(a+b)T=aT+bT,$$

$$(ab)T=aT\cdot bT,$$

那么变换 T 称为是数域 F 的一个**自同构变换**(简称**自同构**).

再看前面的例子. 在数域 $\mathbf{Q}(\sqrt{2})$ 中任意数均可表成 $a+b\sqrt{2}$ 的形式(a, b 属于 $\mathbf{Q}$)，作变换 S:

$$(a+b\sqrt{2})S=a-b\sqrt{2},$$

则

$$[(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})]S$$
$$=(a_1+b_1\sqrt{2})S+(a_2+b_2\sqrt{2})S,$$
$$[(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})]S$$
$$=(a_1+b_1\sqrt{2})S\cdot(a_2+b_2\sqrt{2})S,$$

所以 S 是数域 $\mathbf{Q}(\sqrt{2})$ 的一个自同构变换.

与置换的乘积的定义相仿，我们规定同一数域 F 上两自同构变换 T_1 与 T_2 的乘积 $T_1\circ T_2$，为先作变换 T_1 然后再作变换 T_2，变换 $T_1\circ T_2$ 不难证明也是一对一的．现在来证明 $T_1\circ T_2$ 也是 F 的自同构变换．

设 $a, b\in F$，则

$$(a+b)T_1\circ T_2=[(a+b)T_1]T_2=(aT_1+bT_1)T_2$$
$$=(aT_1)T_2+(bT_1)T_2=aT_1\circ T_2+bT_1\circ T_2,$$
$$(ab)T_1\circ T_2=(abT_1)T_2=(aT_1\cdot bT_1)T_2$$
$$=(aT_1)T_2(bT_1)T_2=(aT_1\circ T_2)(bT_1\circ T_2).$$

根据自同构变换的定义，$T_1\circ T_2$ 是 F 上的一个自同构变换．

我们来证明，一个数域 F 的全体自同构变换 G 按照上面规定的乘法构成一个群——数域 F 的**自同构变换群**，简称**自同构群**．

G 满足群的定义(§3.3)中的(1)，(2)，(4)是显然的．因为自同构变换 T 是一对一的，逆变换 T^{-1} 的存在也是明显的．所需证明的只是 T^{-1} 也是一个自同构变换：

设 a, b 属于 F，自同构变换 T 将 a、b 变为 a', b'：

$$aT=a',\ bT=b',$$

则 T 的逆变换 T^{-1} 将 a', b' 变为 a, b：

$$a'T^{-1}=a,\ b'T^{-1}=b.$$

且

$$(a'+b')T^{-1}=(aT+bT)T^{-1}=[(a+b)T]T^{-1}$$
$$=(a+b)T\circ T^{-1}=a+b=a'T^{-1}+b'T^{-1}$$
$$(a'b')T^{-1}=(aT\cdot bT)T^{-1}=(abT)T^{-1}=ab=a'T^{-1}\cdot b'T^{-1}.$$

所以 T^{-1} 也是 F 的自同构变换，故 T^{-1} 亦属于 G.

现设 T 为数域 F 上的自同构变换，则我们已知 F 必包含有理数域 $\mathbf{Q}$(见§4.1)，我们来证明在变换 T 作用下，任何

有理数必不变：

先证 $0\cdot T=0$. 这是因为任取一数 a 属于 F, 则一方面

$$(a+0)T=aT+0T,$$

另一方面由 $a+0=a$, 可得 $(a+0)T=aT$,

故得

$$aT+0T=aT,$$

即

$$0T=0.$$

其次再证 $1T=1$. 任取一数 b 属于 F, $b\neq 0$, 则由于自同构变换是一对一的, 所以 $bT\neq 0$. 因为 $b=b\cdot 1$, 所以

$$bT=(b\cdot 1)T=bT\cdot 1T,$$

故得

$$1T=1.$$

再证 $nT=n$ 及 $(-n)T=-n$, (这里 n 为任意自然数)

$$nT=(\underbrace{1+1+\cdots+1}_{n\text{个}1})T=\underbrace{1T+1T+\cdots+1T}_{n\text{个}}$$

$$=\underbrace{1+1+\cdots+1}_{n\text{个}}=n,$$

又因

$$n+(-n)=0,$$

所以

$$[n+(-n)]T=0T=0,$$

而

$$[n+(-n)]T=nT+(-n)T=n+(-n)T,$$

所以

$$(-n)T=-n.$$

最后证 $\left(\frac{p}{q}\right)T=\frac{p}{q}$ (这里 p, q 为任意整数, $q\neq 0$).

因

$$q\cdot\frac{p}{q}=p,$$

所以

$$p=pT=\left(q\cdot\frac{p}{q}\right)T=qT\left(\frac{p}{q}\right)T=q\cdot\left(\frac{p}{q}\right)T,$$

所以

$$\left(\frac{p}{q}\right)T=\frac{p}{q}.$$

总之, 这就证明了在自同构变换 T 作用下有理数必不变.

若 K 是 F 的一个扩域，我们来考虑 K 的自同构群 G 中使 F 的元素保持不变的那些自同构变换全体所成的集合 H（也就是 G 中那些满足对一切 a 属于 F 均有 $aT=a$ 的自同构变换 T 的全体）.

容易验证 H 是 G 的一个子群. 我们称 H 为数域 K 在其子域 F 上的自同构群. H 这个群使 F 中的任意元不变，那么使域 K 中的元如何变化呢？我们有下面的重要定理：

定理 数域 K 在其子域 F 上的自同构群中的任一自同构变换，必将 K 的一个元素 u 变为它在 F 上的某一个共轭元素 uT.

证 这条定理实际上也就是说，u 与 uT 要满足 F 上同一个不可约方程(见域 F 上共轭数的定义).

为此，设 u 满足 F 上不可约方程

$$x^n+b_{n-1}x^{n-1}+\cdots+b_0=0,\ (b_0,\ \cdots,\ b_{n-1}\ 属于\ F)$$

设 T 为使 F 中元素不变的 K 的一个自同构变换，则

$$\begin{aligned}0=0\cdot T&=(u^n+b_{n-1}u^{n-1}+\cdots+b_1u+b_0)T\\&=u^nT+(b_{n-1}u^{n-1})T+\cdots+(b_1u)T+b_0T\\&=u^nT+(b_{n-1}T)(u^{n-1})T+\cdots+(b_1T)(uT)+b_0T\\&=(uT)^n+b_{n-1}(uT)^{n-1}+\cdots+b_1(uT)+b_0,\end{aligned}$$

这就是说 uT 亦满足不可约方程

$$x^n+b_{n-1}x^{n-1}+\cdots+b_0=0,$$

即 u 与 uT 在 F 上共轭.

[例 1] 考察有理数域 $\mathbf{Q}$ 上不可约方程 x^4-2x^2+9 的根域 $K=\mathbf{Q}(\sqrt{2},\ i)$. (见 62 页例 5)

显然 $F=\mathbf{Q}(i)$ 是 K 与 $\mathbf{Q}$ 的中间域，它是由 Q 添加不可约方程 $x^2+1=0$ 的根而生成的. $\mathbf{Q}(\sqrt{2},\ i)$ 是由 $F=\mathbf{Q}(i)$ 添加 $\sqrt{2}$ 而生成，而 $\sqrt{2}$ 则满足 $\mathbf{Q}(i)$ 上不可约方程 x^2-2

$=0$, 所以

$$[\mathbf{Q}(i):\mathbf{Q}]=2,\ [\mathbf{Q}(\sqrt{2},\ i):\mathbf{Q}(i)]=2,$$

因此

$$\begin{aligned}[\mathbf{Q}(\sqrt{2},\ i):\mathbf{Q}] &= [\mathbf{Q}(\sqrt{2},\ i):\mathbf{Q}(i)][\mathbf{Q}(i):\mathbf{Q}]\\ &=2\times2=4.\end{aligned}$$

$\mathbf{Q}(\sqrt{2},\ i)$ 中任一数均可用 $1,\ \sqrt{2},\ i,\ \sqrt{2}i$ 的线性组合唯一表出：

$$a+b\sqrt{2}+ci+d\sqrt{2}i\quad (a,\ b,\ c,\ d \text{ 属于 } Q).$$

$\mathbf{Q}(\sqrt{2},\ i)$的一个自同构变换 S：

$$(a+b\sqrt{2}+ci+d\sqrt{2}i)S=a-b\sqrt{2}+ci-d\sqrt{2}i,$$

显然保持 $\mathbf{Q}(\sqrt{2},\ i)$ 的子域 $\mathbf{Q}(i)$ 中的数不变. 类似地, $\mathbf{Q}(\sqrt{2},\ i)$的另一自同构变换 T：

$$(a+b\sqrt{2}+ci+d\sqrt{2}i)T=a+b\sqrt{2}-ci-d\sqrt{2}i,$$

显然保持 $\mathbf{Q}(\sqrt{2},\ i)$的子域$\mathbf{Q}(\sqrt{2})$中的数不变. 根据变换乘积的定义知 S 与 T 的乘积 ST 也是 $\mathbf{Q}(\sqrt{2},\ i)$ 的一个自同构变换. 因此我们有了 $\mathbf{Q}(\sqrt{2},\ i)$的四个自同构变换:

$$S,\ T,\ ST,\ I\quad (\text{恒等变换}).$$

它们对 $\sqrt{2}$ 与 i 这两个数的作用可列表如下：

$$\begin{cases}(\sqrt{2})S=-\sqrt{2}\\ (i)S=i\end{cases},\quad \begin{cases}(\sqrt{2})T=\sqrt{2}\\ (i)T=-i\end{cases},$$

$$\begin{cases}(\sqrt{2})ST=-\sqrt{2}\\ (i)ST=-i\end{cases},\quad \begin{cases}(\sqrt{2})I=\sqrt{2}\\ (i)I=i\end{cases}.$$

$\mathbf{Q}(\sqrt{2},\ i)$的自同构群就是由 $I,\ S,\ T,\ ST$ 这四个自同构变换组成. 这是因为, 由本节定理1知道 $\mathbf{Q}(\sqrt{2},\ i)$ 的任意一个自同构变换 U, 必将 $\sqrt{2}$ 变为 $\mathbf{Q}$ 上的共轭数 $\sqrt{2}$ 或 $-\sqrt{2}$, 将 i 变成 $\mathbf{Q}$ 上的共轭数 i 或 $-i$, 所在 U 必为 $I,\ S,\ T,\ ST$ 四者之一. 容易验证 $I,\ S,\ T,\ ST$ 这四个自同构变换

之间的乘积满足：

$$S^2=I,\ T^2=I,\ ST=TS,\ STST=SSTT=I.$$

且 $\mathbf{Q}(\sqrt{2},\ i)$ 在子域 $\mathbf{Q}(\sqrt{2})$ 上的自同构群由 $I,\ T$ 两个自同构组成. $\mathbf{Q}(\sqrt{2},\ i)$ 在子域 $\mathbf{Q}(i)$ 上的自同构群由 $I,\ S$ 两个自同构组成.

5. 代数方程的伽罗华群

现在我们可以来定义一个代数方程的伽罗华群了. 它是决定一个方程是否能用代数方法求解的关键.

定义 设有数域 F 上的方程 $f(x)=0$, 数域 N 是方程 $f(x)=0$ 的根域, 则称 N 在 F 上的自同构群为方程 $f(x)=0$ 的伽罗华群.

现在来看一个具体的例子.

$x^4-3=0$ 是有理数域 $\mathbf{Q}$ 上的一个不可约方程. 它有四个根：

$$\sqrt[4]{3},\quad i\sqrt[4]{3},\quad -\sqrt[4]{3},\quad -i\sqrt[4]{3}.$$

其根域 $\quad N=\mathbf{Q}(\sqrt[4]{3},\ i\sqrt[4]{3},\ -\sqrt[4]{3},\ -i\sqrt[4]{3})$

也可由 $\mathbf{Q}$ 添加 $\sqrt[4]{3}$ 与 i 而生成, 所以又有

$$N=\mathbf{Q}(\sqrt[4]{3},\ i).$$

显然 $\quad [\mathbf{Q}(\sqrt[4]{3}):Q]=4,\quad [\mathbf{Q}(\sqrt[4]{3},\ i):\mathbf{Q}(\sqrt[4]{3})]=2.$

所以 $$[\mathbf{Q}(\sqrt[4]{3},\ i):\mathbf{Q}]=4\times2=8.$$

容易看出 $N=\mathbf{Q}(\sqrt[4]{3},\ i)$ 中任一数均可用 $1,\ \sqrt[4]{3},\ \sqrt{3},\ \sqrt[4]{27},\ i,\ i\sqrt[4]{3},\ i\sqrt[4]{3},\ i\sqrt[4]{27}$ 八个数的线性组合唯一表出：

$$a_1+a_2\sqrt[4]{3}+a_3\sqrt[4]{3}+a_4\sqrt[4]{27}+a_5 i$$
$$+a_6 i\sqrt[4]{3}+a_7 i\sqrt{3}+a_8 i\sqrt[4]{27}.$$

这里 $a_1,\ a_2,\ \cdots,\ a_8$ 属于 $\mathbf{Q}$.

显然，对 N 的任一自同构变换 T 来说，只要知道了 $(\sqrt[4]{3})T$ 与 $(i)T$ 等于什么，T 就完全确定了．与第 73 页的例类似可知，N 在 F 上的自同构变换必将 $\sqrt[4]{3}$ 变为其四个共轭数 $\sqrt[4]{3}$，$-\sqrt[4]{3}$，$i\sqrt[4]{3}$，$-i\sqrt[4]{3}$ 之一(即 $\mathbf{Q}$ 上不可约方程 $x^4-3=0$ 的根)也必将 i 变为其两个共轭数 i，$-i$ 之一(即 $\mathbf{Q}$ 上不可约方程 $x^2+1=0$ 的根)，所以若令

$$S:\ \begin{cases}\sqrt[4]{3}\,S=i\sqrt[4]{3}\\ iS=i,\end{cases}\qquad T:\ \begin{cases}\sqrt[4]{3}\,T=\sqrt[4]{3}\\ iT=-i.\end{cases}$$

则 N 在数域 $\mathbf{Q}$ 中的伽罗华群由以下八个自同构变换所构成：

$$I,\ S,\ S^2,\ S^3,\ T,\ TS,\ TS^2,\ TS^3.$$

它们对 $\sqrt[4]{3}$ 和 i 的作用如下表：

	I	S	S^2	S^3	T	TS	TS^2	TS^3
$\sqrt[4]{3}$ 变为	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$
i 变为	i	i	i	i	$-i$	$-i$	$-i$	$-i$

现在我们来更详细地看一下，这个伽罗华群

$$G=\{I,\ S,\ S^2,\ S^3,\ T,\ TS,\ TS^2,\ TS^3\}$$

与用代数方法求解方程 $x^4-3=0$ 的关系是怎样的？

G 有一子群 $H=\{I,\ S,\ S^2,\ S^3\}$ 它是一个由 S 的乘幂所生成的循环群．H 又有一子群 $L=\{I,\ S^2\}$ 它也是一个循环群．H 中的变换使 i 保持不变，因而也使 $\mathbf{Q}(i)$ 中每一数不变．而 L 则使数域 $\mathbf{Q}(i,\ \sqrt{3})$ 中的每一数保持不变．由此可见随着群的不断缩小：

$$G\supset H\supset L\supset I,$$

相应不变的数域就不断扩大：

$$\mathbf{Q}\subset\mathbf{Q}(i)\subset\mathbf{Q}(i,\ \sqrt{3})\subset\mathbf{Q}(i,\ \sqrt[4]{3}),$$

而在这一列数域中，后一数域都是由前一数域分别添加简单方程 $x^2+1=0$，$y^2-3=0$，$z^2-\sqrt{3}=0$ 的根而生成的．这些简单方程都可以直接开方来求解．因而 $\mathbf{Q}(i)$ 中的数可以由 $\mathbf{Q}$ 中的数经有理运算和开方得出．$\mathbf{Q}(i,\sqrt{3})$中的数又可由 $\mathbf{Q}(i)$，从而归根结底可由 $\mathbf{Q}$ 中的数经有理运算及开方求得，…．如此继续，就知道 $\mathbf{Q}(i,\sqrt[4]{3})$中的一切数包括原方程 $x^4-3=0$ 的一切根都可以由 $\mathbf{Q}$ 中的数经开方和加、减、乘、除来求得．

这个例子更具体地告诉我们伽罗华群的子群与代数方程求解问题之间的密切关系．这个问题的最后解决我们放在下一章里．

6．求代数方程的伽罗华群的具体方法

上面我们看出一个代数方程的伽罗华群的重要性．虽然伽罗华群的定义是很明确的，但是要根据这个定义去具体确定一个代数方程的伽罗华群是困难的．下面我们要来介绍一种具体确定伽罗华群的方法，它在很多情况下是比较方便的．

设有数域 F 上的方程 $f(x)=0$，数域 N 是 $f(x)=0$ 的根域，G 是 $f(x)=0$ 的伽罗华群，则由73页定理知道：G 中任一变换 T 必将 $f(x)=0$ 的根变为 $f(x)=0$ 的根，而且原来不同的根变换后仍是不相同的．若 $f(x)=0$ 为 n 次方程，它有 k个不同的根 u_1，u_2，…，u_k，则

$$u_1T=u_{\alpha_1},\ u_2T=u_{\alpha_2},\ \cdots,\ u_kT=u_{\alpha_k}.\quad (k\leqslant n)$$

这里 α_1，α_2，…，α_k 是 1，2，…，k 的一种排列．另一方面 N 中任一数 W 必可表成系数属于 F 的 u_1，u_2，…，u_k 的多项式：

$$W=h(u_1, u_2, \cdots, u_k).$$

因为 F 中的数在 T 作用下不变，所以

$$WT=[h(u_1, u_2, \cdots, u_k)]T=h(u_1T, u_2T, \cdots, u_kT)$$
$$=h(u_{\alpha_1}, u_{\alpha_2}, \cdots, u_{\alpha_k}).$$

所以 T 在 W 上的作用，完全由 T 在 $u_1, u_2, \cdots, u_k$ 上的作用所唯一确定．因此我们得到下面的定理：

定理 设 $f(x)=0$ 是数域 F 上的一个 n 次方程，它有 k 个不同的根 $u_1, u_2, \cdots, u_k$，其根域 $N=F(u_1, u_2, \cdots, u_k)$．于是 $f(x)=0$ 的伽罗华群 G 中任一自同构变换 T 确定一置换

$$\begin{pmatrix}1 & 2\cdots k\\ \alpha_1 & \alpha_2\cdots\alpha_k\end{pmatrix},$$

而且反过来这一置换完全确定了 T．

但是要注意的是：反过来并不是任意一个置换

$$\begin{pmatrix}1 & 2\cdots k\\ \alpha_1 & \alpha_2\cdots\alpha_k\end{pmatrix}$$

都对应着伽罗华群中的一个自同构变换．这是因为伽罗华群中的自同构变换，使 F 不变，所以如果根的一个多项式的值在 F 中，则该自同构将使这一多项式的值不变．这样一来 $k!$ 个置换

$$\begin{pmatrix}1 & 2\cdots k\\ \alpha_1 & \alpha_2\cdots\alpha_k\end{pmatrix}$$

中只有满足上述要求的一部分置换，才与伽罗华群中的变换成一一对应，所以伽罗华群可以看成是由这些置换所成的置换群．现在问题是如何来决定这个置换群？

对于文字系数的一般 n 次方程

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0,$$

它的 n 个根 $x_1, x_2, \cdots, x_n$ 是相互独立的，所以它的伽罗华群

显然就是所有 $n!$ 个置换所构成的对称群 S_n.

因此对于一个系数在数域 F 中的具体方程, 若方程的根的任一多项式(系数属于 F)的值在 F 中, 则此方程在 F 中的伽罗华群 G 所对应的根的置换, 应不改变此多项式的值. 若此多项式的值不在 F 中, 则必有 G 中一变换它所对应的根的置换要改变此多项式之值. 利用上面的性质, 就可以寻找一些方程的伽罗华群了.

[例 1] 讨论二次方程 $x^2+3x+1=0$ 的伽罗华群.

解 要指出的是求伽罗华群时首先要明确方程是在什么域上. 现在这个方程有两个根 x_1 与 x_2, 所有可能的置换只有

$$\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix} \text{ 与 } \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix},$$

所以这个方程的伽罗华群只有两种可能:

或者是 $\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ 或者是 $\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ 与 $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$,

要看是在什么数域上而定.

现取函数 x_1-x_2, 我们知道

$$x_1-x_2=\sqrt{3^2-4}=\sqrt{5}.$$

如果我们把这一方程作为有理数域 $\mathbf{Q}$ 上的方程, 则此多项式之值 $\sqrt{5}$ 不在 $\mathbf{Q}$ 中, 所以相应的伽罗华群中应有一置换能改变其值, 这只有 $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$ 这个置换. 所以方程 $x^2+3x+1=0$ 在有理数域 Q 中的伽罗华群必包含置换 $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$, 即这时伽罗华群是由 $\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ 与 $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$ 这两个置换所组成.

如果此方程作为实数域 $\mathbf{R}$ 上的, 则因 $\sqrt{5}$ 在实数域 $\mathbf{R}$ 中,

所以群中一切置换都不应改变 x_1-x_2 之值. 这样 $\begin{pmatrix}1&2\\2&1\end{pmatrix}$ 这个置换不能在此群中. 故方程 $x^2+3x+1=0$ 在实数域 $\mathbf{R}$ 中的伽罗华群仅由 $\begin{pmatrix}1&2\\1&2\end{pmatrix}$ 这个恒等置换所构成.

这个例子说明, 在寻找伽罗华群时必须首先说明是什么域上的方程.

[例 2] 讨论 $\mathbf{Q}$ 上的方程 $x^3-3x+1=0$ 的伽罗华群.

解 它有三个根 x_1, x_2, x_3, 所以至多有六种置换:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

为了求这个方程的伽罗华群 G, 我们利用多项式 $(x_1-x_2)\times(x_2-x_3)(x_3-x_1)$, 由第 7 页(1.22)式知, 对于方程 $x^3-3x+1=0$ 的三个根 x_1, x_2, x_3, 有

$$(x_1-x_2)(x_2-x_3)(x_3-x_1)=\sqrt{-4\times(-3)^3-27\times1^2}$$
$$=\sqrt{108-27}=\sqrt{81}=9,$$

9 是有理数, 所以群 G 中一切置换都应使这多项式的值不变. 但上面六个置换中只有

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

这三个置换不改变它的值. 所以群 G 的元素或者就是这三个置换, 或者只是一个恒等置换 $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$. 所以单利用 $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ 还未能完全确定群 G.

我们再应用另外一个根的多项式 x_1, 如果群 G 只有一

个置换$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，那么$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$当然不会改变$x_1$的值，所以$x_1$必在有理数域中．换句话说，这三次方程式的根$x_1$必须是有理数．根据同样的道理知$x_2$，$x_3$也必须是有理数．但方程$x^3-3x+1=0$没有有理数根①．所以群$G$不能单含$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$这个置换．故方程$x^3-3x+1=0$在有理数域$Q$中的伽罗华群由

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

这三个置换所构成．

［例3］　求$\mathbf{Q}$上的方程$x^3-2=0$的伽罗华群G．

解　与例2一样可证这个方程没有有理数根．设这个方程的三个根为x_1，x_2，x_3，所以至多有六种置换．

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ a=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ b=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$

$$c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ d=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ e=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

由此六个置换共可构成6个群：

---

① 这个方程不可能有分数根的证明是不难的，若不然，设有根$\frac{p}{q}$（这里p与q是互素的整数），则

$$\frac{p^3}{q^3}-3\frac{p}{q}+1=0$$

即
$$p^3-3pq^2+q^3=0$$

于是q能除尽p，这与p，q互素矛盾．于是此方程只可能有整数根．但方程的常数项等于1，所以其根只可能是±1这两个因子，但验证下来±1都不是根，所以方程$x^3-3x+1=0$没有有理根．

$$G_1=\{I\},\qquad G_2=\{I,\ a\},$$
$$G_3=\{I,\ b\},\qquad G_4=\{I,\ c\},$$
$$G_5=\{I,\ d,\ e\},\ S_3=\{I,\ a,\ b,\ c,\ d,\ e\}.$$

因 x_1 不是有理数，所以 G 不可能是 G_4（因为 G_4 中不包含使 x_1 改变其值的置换）. 同样，由于 x_2, x_3 不是有理数，所以 G 也不可能是 G_2, G_3，当然也不可能是 G_1. 再看多项式

$$(x_1-x_2)(x_2-x_3)(x_3-x_1)=\sqrt{-4\times0^3-27\times2^2}=6\sqrt{-3}$$

的值也不是有理数，所以 G 也不可能是 G_5（因为 G_5 中的所有置换均不改变 $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ 的值），因此 $\mathbf{Q}$ 上的方程 $x^3-2=0$ 的伽罗华群 G 必为 S_3，即所有六种置换所构成的对称群.

五、代数方程的代数解法．尺规作图问题

1. 尺规作图问题

在平面几何中，大家都知道著名的尺规作图三个不可能问题．这就是有限次地使用直尺与圆规不可能实现：

(1) 三等分任意角(三等分角)，

(2) 作一立方体使其体积为已知立方体之两倍(倍立方)，

(3) 作一正方形使其面积等于已知圆的面积(化圆为方).

下面我们来证明(1)、(2)的不可能．(3)的不可能证明涉及圆周率 π 的超越性，本书无法进行讨论.

我们知道仅用直尺和圆规当然只能作直线和圆．而从解析几何知道它们分别是一次方程和二次方程的轨迹．而求直线与直线、直线与圆、或圆与圆的交点的问题，从代数上看来不过是解一次方程或二次方程组的问题，可以证明，最后的解是可以从方程的系数(已知量)经过有限次的加、减、乘、除和开平方求得．从另一方面讲，我们在平面几何中也确实知道，假使给定了两线段 a、b 和单位长度，可以用直尺和圆规作出它们的和 $a+b$，差 $a-b$，积 ab，商 $\frac{a}{b}$，以及这些量的平方根等．因此，一个几何量能否用直尺圆规作出的问题，等价于它能否由已知量经过加、减、乘、除、开方运算求得．

为了证明一般的三等分角不可能，我们只需证明一个特别的角不能用圆规和直尺三等分就行了．

我们取 $120°$ 这个角来看．在给出了单位长度的条件下，作出 $120°$ 的三等分即 $40°$ 角的充分必要条件，是要能作出长为 $\cos 40°$ 的线段(为什么，请想一想)．利用三角恒等式：

$$2\cos 3\alpha=8\cos^3\alpha-6\cos\alpha,$$

则有

$$2\cos 120°=8\cos^3 40°-6\cos 40°,$$

因为 $\cos 120°=-\frac{1}{2}$，代入后即知 $\cos 40°$ 应是

$$8y^3-6y-1=0$$

的根．设 $x=2y$，则上述方程又成为

$$x^3-3x+1=0. \tag{5.1}$$

因此用直尺、圆规三等分 $120°$ 角的问题，等价于：从有理数域出发利用加、减、乘、除、开平方运算能否求得方程(5.1)的根．

为此我们先来证明一条定理：

定理 若 $p(x)$ 是数域 F 上的一个不可约三次多项式，K 是 F 的扩张域，且 $[K:F]=2^m$，则 $p(x)$ 在 K 上也不可约.

证明 利用反证法，如果 $p(x)$ 在 K 上可约，那末 $p(x)$ 可表成两个 K 上的多项式的乘积：$p(x)=q(x)r(x)$，其中 $q(x)$、$r(x)$ 必有一个是一次多项式 $x-u$，所以 K 必须至少含有 $p(x)=0$ 的一个根 u，又因 $p(x)$ 在 F 上不可约，所以 $[F(u):F]=3$. 但由第63页的系知道 $[F(u):F]$ 应能整除 $[K:F]=2^m$，这是不可能的. 故定理证毕.

由这条定理就可知道一个不可约的三次方程是不可能通过有限次加、减、乘、除和开平方来求解的. 因为逐次将平方根添加于 F 时所生成的扩张域 $K=F(\sqrt{a},\ \sqrt{b},\ \sqrt{c},\ \cdots)$ 对于 F 的维数 $[K:F]$ 必为 2^m，而由上面的定理知道，这个扩张域中是不可能含有这个三次方程的根.

而我们已经知道三次方程 $x^3-3x+1=0$ 在有理域中是不可约的(见81页，例2). 所以这个三次方程是不能通过有限次加、减、乘、除与开平方来求解的.

这就证明了，有限次地使用直尺和圆规不能将 $120°$ 角三等分的，从而三等分任意角是不可能的.

用完全类似的方法可以证明，仅用直尺和圆规是不能解决倍立方问题的. 因为若将已知立方体的边长取作为单位，设要求作的立方体的边长为 x，则因新立方体的体积($=x^3$)应是原来立方体体积($=1$)的二倍，所以

$$x^3=2 \tag{5.2}$$

但这个三次方程在有理域中也是不可约的. 因此由上面的定理知道，它不可能用加、减、乘、除与开平方运算来求解. 这就证明了倍立方问题也是不能用直尺和圆规解决的.

2. 代数方程可用代数方法求解的准则

现在我们可以来讨论本书的中心问题了：怎样的方程才可以用代数方法来求解？

伽罗华彻底解决了这个问题．他给出了下面的判断准则：

定理 一个 $F=\mathbf{Q}(a_1, \cdots, a_n)$ 上的代数方程

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0, \tag{5.3}$$

当且仅当它的伽罗华群是一个可解群时，此方程可用代数方法求解．

我们不打算对伽罗华的准则给出严格的证明，只准备对他的理论的主要思路给出一个较通俗的阐述．

我们知道，"一个方程能用代数方法求解"与"它的根域 N 可由 F 经过有限次添加根式而生成"这件事是等价的．这样每次添加一个根式所生成的扩域 K_i，形成一列插在 F 与 N 之间的中间域：

$$F=K_0\subset K_1\subset K_2\cdots\subset K_s=N \tag{5.4}$$

这里每一个 K_{i+1} 是由 K_i 添加一个根式 a_i^{1/r_i} 所生成的扩域（a_i 属于 K_i），即 $K_{i+1}=K_i(a_i^{1/r_i})$．而且因为若 $r=st$，则 $a^{1/r}=a^{1/st}=(a^{1/s})^{1/t}$，所以不妨设所有 r_i 都是素数．可以证明：1 的任意次根均可由有理数经有限次加、减、乘、除与开方运算求得，所以我们不妨先将所有 1 的各次方根添加到 F 中去而生成一扩域，为简单起见不妨仍记此扩域为 F，也就是说 F 是包含方程的系数及 1 的各次根的最小数域．这不影响方程能否用代数方法求解问题的讨论．

我们知道方程 $x^{r_i}=a_i$ 的根，除 a_i^{1/r_i} 外，还有 $\zeta a_i^{1/r_i}$，$\zeta^2 a_i^{1/r_i}$，

$\cdots$, $\zeta^{r_i-1}a_i^{1/r_i}$, 这里 ζ 是 1 的 r_i 次原根①. 这些与 a_i^{1/r_i} 共轭的根显然也都属于 K_{i+1}(因 ζ 已经属于 F), 所以 K_{i+1} 是 K_i 上的方程 $x^{r_i}-a_i=0$ 的根域, 因而是 K_i 的正规扩张域. 所以(5.4)中一列扩张域 K_1, K_2, K_3, $\cdots$, K_S 都是正规扩张. 而且

$$[K_1:F]=r_1,\ [K_2:K_1]=r_2,\ \cdots,\ [K_S:K_{S-1}]$$
$$=[N:K_{S-1}]=r_{S-1}$$

都是素数.

现在我们根据正规扩张域序列 (5.4) 来分析一下, N 在 F 上的自同构群(即方程(5.3)的伽罗华群)G 的结构.

因为群 G 是使 F 中的数不变的、N 的一切自同构变换所成的群. 而 $N\supset K_1\supset F$, 所以使 K_1 中的数不变的、N 的一切自同构变换, 当然也使 F 中的数不变. 故域 N 在 K_1 上的自同构群 (记为 G_1) 是 G 的子群, 而且由于 K_1 是 F 的正

① 我们称方程 $x^n-1=0$ 的 n 个根为 n 次单位根. 方程 $x^n-1=0$ 的 n 个根的三角函数形式可以表示成:

$$1,\ \zeta=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n},\ \zeta^2=\cos\frac{4\pi}{n}+i\sin\frac{4\pi}{n},\ \cdots,$$

$$\zeta^k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\ \cdots,\ \zeta^{n-1}=\cos\frac{2(n-1)\pi}{n}+i\sin\frac{2(n-1)\pi}{n},$$

这 n 个单位根中当 k 与 n 互素时有 $(\zeta^k)^l\neq 1\ (l=1,2,\cdots,n-1)$, 这时 ζ^k 就称为是 n 次原单位根, 简称原根. 例如, 当 $n=3$,

$$\omega=\frac{-1+\sqrt{3}i}{2}\quad 及\quad \omega^2=\frac{-1-\sqrt{3}i}{2}$$

都是原根, 而 1 则不是. 当 $n=4$ 时,

$$\zeta=\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}=i\quad 与\quad \zeta^3=\cos\frac{3\pi}{4}+i\sin\frac{3\pi}{4}=-i$$

都是 1 的原根. 而 1 和 $\zeta^2=\cos\pi+i\sin\pi=-1$ 则不是.

如果求得了一个 n 次原根 ζ^k, 则其所有的 n 次单位根都可用 ζ^k 的幂来表示. 因此要求所有 n 次单位根, 就只要先求得它的一个 n 次原根即可.

规扩域，可以证明 G_1 一定是 G 的不变子群，并且

$$\frac{G\text{ 的阶数}}{G_1\text{ 的阶数}}=[K_1:F]=r_1.$$

仿此，使 K_2 中的数不变的 N 的一切自同构变换全体构成 G_1 的不变子群 G_2，且

$$\frac{G_1\text{ 的阶数}}{G_2\text{ 的阶数}}=[K_2:K_1]=r_2;$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots;$$

使 K_{S-1} 中的数不变的 N 的一切自同构变换全体构成 G_{S-1} 的不变子群 G_S，且

$$\frac{G_{S-1}\text{ 的阶数}}{G_S\text{ 的阶数}}=[N:K_{S-1}]=r_S.$$

因此由上述的正规扩张域序列

$$F=K_0\subset K_1\subset K_2\subset\cdots\subset K_S=N;$$

$$[K_1:F]=r_1,\ [K_2:K_1]=r_2,\ \cdots,\ [K_{S-1}:K_{S-2}]=r_{S-1},$$

$$[N:K_{S-1}]=r_S;$$

诱导出方程(5.3)的伽罗华群的一列不变子群序列：

$$G\supset G_1\supset G_2\cdots\supset G_S=I \tag{5.5}$$

$$\frac{G\text{ 的阶数}}{G_1\text{ 的阶数}}=r_1,\ \frac{G_1\text{ 的阶数}}{G_2\text{ 的阶数}}=r_2,\ \cdots,\ \frac{G_{S-1}\text{ 的阶数}}{G_S\text{ 的阶数}}=r_S$$

而且由于 $r_1, r_2, \cdots, r_S$ 都是素数，所以对每一个 i 而言，G_i 都是 G_{i-1} 的极大不变子群. 所以(5.5)就是合成群列，$r_1, r_2, \cdots, r_S$ 就是群 G 的组合因数.

这就阐明了为什么一个方程若可用代数方法求解，则它在系数域中的伽罗华群 G 的组合因数都是素数，也就是说 G 是可解群.

现在我们要反过来阐明，若一个方程在其系数域中的伽罗华群是可解群，则此方程必可用代数方法求解.

先看一个特殊情况：若 F 上的方程

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n=0 \qquad (5.6)$$

的次数 n 是素数，它的伽罗华群是由下列形式的置换所构成的循环群：

$$G=\{I,\ a\ ,\ a^2,\ a^3,\ \cdots,\ a^{n-1}\},$$

其中

$$a=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ 2 & 3 & \cdots & n & 1\end{pmatrix}.$$

这个群是一个可解群，它的合成群列是

$$G\supset I.$$

设方程 (5.6) 的 n 个根为 $x_1,\ x_2,\ \cdots,\ x_n$；则在此情况下这 n 个根可用下法求得：

令 ζ 为 1 的 n 次原根．考察方程组

$$\begin{cases}x_1+x_2+x_3+\cdots+x_n=r_0=-a_1,\\ x_1+\zeta x_2+\zeta^2x_3+\cdots+\zeta^{n-1}x_n=r_1,\\ x_1+\zeta^2x_2+\zeta^4x_3+\cdots+\zeta^{2(n-1)}=r_2,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ x_1+\zeta^{n-1}x_2+\zeta^{2(n-1)}x_3+\cdots+\zeta^{(n-1)^2}x_n=r_{n-1}.\end{cases} \qquad (5.7)$$

任取方程组(5.7)中的一个方程来看：

$$x_1+\zeta^kx_2+\zeta^{2k}x_3+\cdots+\zeta^{(n-1)k}x_n=r_k,$$

将置换

$$a=\begin{pmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ 2 & 3 & 4 & \cdots & n & 1\end{pmatrix}$$

作用于上述方程之左端，就变成：

$$x_2+\zeta^kx_3+\zeta^{2k}x_4+\cdots+\zeta^{(n-1)k}x_1,$$

这和用 ζ^{-k} 乘方程的左端的结果是一样的（因为 $\zeta^n=1$，所以 $\zeta^{-k}=\zeta^{nk}\zeta^{-k}=\zeta^{nk-k}=\zeta^{(n-1)k}$）．所以

$$x_2+\zeta^kx_3+\zeta^{2k}x_4+\cdots+\zeta^{(n-1)k}x_1=r_k\zeta^{-k},$$

因此置换 $$a=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ 2 & 3 & \cdots & n & 1\end{pmatrix}$$

将 r_k 变为 $r_k\zeta^{-k}$，而 $(r_k)^n=(r_k\zeta^{-k})^n$，所以置换 a 不改变 $(r_k)^n$ 之值。由于群 G 中之置换都是 a 之乘幂所组成，所以群 G 中之一切置换都不改变 $(r_k)^n$ 之值。因而 $(r_k)^n$ 必为 F 中之数，即令 $(r_k)^n=\alpha_k$，则 α_k 属于 F，也即 $r_k=\sqrt[n]{\alpha_k}$。所以方程组(5.7)可写成：

$$\begin{cases} x_1+x_2+\cdots+x_n=-a_1, \\ x_1+\zeta x_2+\zeta^2x_3+\cdots+\zeta^{n-1}x_n=\sqrt[n]{\alpha_1}, \\ x_1+\zeta^2x_2+\zeta^4x_3+\cdots+\zeta^{2(n-1)}x_n=\sqrt[n]{\alpha_2}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1+\zeta^{n-1}x_2+\zeta^{2(n-1)}x_3+\cdots+\zeta^{(n-1)^2}x_n=\sqrt[n]{\alpha_{n-1}}. \end{cases} \tag{5.8}$$

(这里 α_1, α_2, $\cdots$, α_{n-1} 均为 F 中的数)

因为 (5.8) 是 x_1, x_2, $\cdots$, x_n 的线性方程组，所以只要对 $\zeta^1,\zeta^2,\cdots,\zeta^{(n-1)^2}$, $\sqrt[n]{\alpha_1}$, $\sqrt[n]{\alpha_2}$, $\cdots$, $\sqrt[n]{\alpha_{n-1}}$ 作有理运算(加、减、乘、除)，即可解得 x_1, x_2, $\cdots$, x_n. 由此可见 x_1, x_2, $\cdots$, x_n 均在 $F(\zeta,\ \sqrt[n]{\alpha_1},\ \sqrt[n]{\alpha_2},\ \cdots,\ \sqrt[n]{\alpha_{n-1}})$ 中，即方程 (5.6) 可用代数方法求解.

[例] **Q** 上的方程

$$x^3-3x+1=0 \tag{5.9}$$

的伽罗华群

$$G=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$$

(见 80 页例 2)，这是阶数为 3 的循环群，所以根据上面的方法，我们可从方程组

$$x_1+x_2+x_3=0$$
$$x_1+\omega x_2+\omega^2x_3=r_1$$

$$x_1+\omega^2x_2+\omega x_3=r_2$$

来求解方程(5.9)的三个根 x_1, x_2, x_3. 这里 ω 表示 1 的三次原根，$\omega=\frac{-1+\sqrt{3}i}{2}$. 而 r_1 与 r_2 则可由系数域（有理数域）中的数经过有理运算及开方运算而得. 事实上，这就是我们以前在第 22 页解三次方程的方法.

对于一般的方程，若它在系数域中的伽罗华群是可解群，亦即有合成群列：

$$G\supset G_1\supset G_2\cdots G_{S-1}\supset G_S=I,$$

这里 G_i 是 G_{i-1} 的极大不变子群($i=1, 2, \cdots, S$)，且

$$\frac{G\text{ 的阶数}}{G_1\text{ 的阶数}}=r_1,\quad \frac{G_1\text{ 的阶数}}{G_2\text{ 的阶数}}=r_2,\quad \cdots,$$

$$\frac{G_{S-1}\text{ 的阶数}}{G_S\text{ 的阶数}}=r_S$$

都是素数，则可以证明其根域 N 与系数域 F 之间也有相应的一列正规中间域：

$$F=K_0\subset K_1\subset K_2\cdots\subset K_S=N,$$

且 $[K_1:F]=r_1$, $[K_2:K_1]=r_2$, $\cdots$, $[N:K_{S-1}]=r_S$.

因为每一 K_{i+1} 是 K_i 的正规扩张，而由第 65 页的定理知道 K_{i+1} 一定是 K_i 上某一方程 $p_i(x)=0$ 的根域. 可以证明 $p_i(x)$ 在域 K_i 中的伽罗华群一定是

$$\left\{I,\ a=\begin{pmatrix}1 & 2 & \cdots & r_{i-1} & r_i\\ 2 & 3 & \cdots & r_i & 1\end{pmatrix},\ a^2,\ \cdots,\ a^{r_i-1}\right\}$$

形式的 r_i 阶循环群，是可解的. 因此由上面介绍的方法知道方程 $p_i(x)=0$ 可用代数方法求解. 也就是说 K_{i+1} 中的数一定可用 K_i 中的数经过有限次加、减、乘、除和开方运算表出，因而根域 N 中的数可用系数域 F 中的数经过有限次加、减、乘、除和开方运算表出. 这就是说方程

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$$

可用代数方法求解.

3. 三次方程的不可约情况

在第8页中我们已看到，当三次方程 $x^3+px+q=0$ 的系数为实数,且其判别式 $\Delta=\frac{1}{4}q^2+\frac{1}{27}p^3<0$ 时，它的三个根是互异的实数．这种情况称为三次方程的不可约情况．但这时求根的卡当公式却由于要对负数开平方而出现了虚数．虽然这些虚数最终可被消去而得到实数根，但对实系数方程的实数根要通过虚数的媒介才能求得，这总使人感到有点别扭．不少数学家花了许多精力想消除在卡当公式中出现的虚数，希望能找到仅含有实数运算的求根公式，可是都失败了．现在利用伽罗华的理论,我们来证明这是不可能的:在这种情况下,不存在不包含虚数的代数求根公式.

我们先来证明两条辅助定理作为准备.

辅助定理1　若三次方程 $y^3+py+q=0$ 在系数域 $F=\mathbf{Q}(p,q)$ 中不可约,它的三个根记为 y_1、y_2、y_3，令 $D=[(y_1-y_2)\times(y_2-y_3)(y_3-y_1)]^2$, $(D=-108\Delta)$则此方程的根域

$$F(y_1,\ y_2,\ y_3)=F(\sqrt{D},\ y_1).$$

证明　由 D 的定义易知: $\sqrt{D}$ 属于 $F(y_1,\ y_2,\ y_3)$，从而 $F(y_1,\ y_2,\ y_3)\supset F(\sqrt{D},\ y_1)$．所以只需证明

$$y_1,\ y_2\in F(\sqrt{D},\ y_1),\ 即\ \ F(y_1,\ y_2,\ y_3)\subset F(\sqrt{D},\ y_1)$$

就行了．因为在域 $F(\sqrt{D},\ y_1)$中，方程 $y^3+py+q=0$ 可分解出一个因子$(y-y_1)$,所以剩下的两次因子

$$(y-y_2)(y-y_3)=y^2-(y_2+y_3)y+y_2y_3$$

的系数亦在$F(\sqrt{D}, y_1)$中，故知

$$(y_1-y_2)(y_1-y_3)=y_1^2-(y_2+y_3)y_1+y_2y_3$$

也在$F(\sqrt{D}, y_1)$中．因而$y_2-y_3=\pm\sqrt{D}/(y_1-y_2)(y_1-y_3)$亦在$F(\sqrt{D}, y_1)$中．由于$y_2-y_3$与$y_2+y_3$均在$F(\sqrt{D}, y_1)$中，所以$y_2$与$y_3$也在其中．

辅助定理2 实域K上的一个素数r次的多项式x^r-a或在K中不可约，或在K中有一根．

证明 将1的r次原根ζ及方程$x^r-a=0$的一个根u添加到K中，得到扩域$K(\zeta, u)$，则$K(\zeta, u)$包含方程$x^r-a=0$的所有r个根：

$$u,\ \zeta u,\ \zeta^2 u,\ \cdots,\ \zeta^{r-1}u.$$

所以在$K(\zeta, u)$中，x^r-a可分解成一次因式的乘积：

$$x^r-a=(x-u)(x-\zeta u)\cdots(x-\zeta^{r-1}u) \qquad (*)$$

若x^r-a在K上有一个次数为$m(1\leqslant m<r)$的因式$g(x)$（即x^r-a在K上可约），则$g(x)$必为$(*)$中m个一次因式的乘积，于是$g(x)$之常数项b必为$x^r-a=0$的m个根的乘积：

$$b=\zeta^{j_1}u\cdot\zeta^{j_2}u\cdot\cdots\cdot\zeta^{j_m}u=\zeta^{j_1+j_2+\cdots+j_m}u^m=\zeta^j u^m,$$

于是
$$b^r=(\zeta^j u^m)^r=(\zeta^r)^j(u^r)^m=(u^r)^m=a^m,$$

因为$m<r$，且与r互素（因r是素数），所以存在整数s、t使

$$sm+tr=1,$$

故
$$b^{sr}=a^{sm}=a^{1-tr}=\frac{a}{a^{tr}},$$

于是$a=(b^s a^t)^r$．因为b与a均为K中的数（b是K上多项式$g(x)$的常数项），所以$b^s a^t$也是K中的数．这就是说K中包含a的一个r次根$b^s a^t$．这就证明了若x^r-a在K中可约，则方程$x^r-a=0$在K中即有一根$b^s a^t$．

现在我们可以来证明本节中的主要定理了．

定理 若实系数三次方程 $y^3+py+q=0$ 的根皆为实数，且在系数域 F 中不可约，则不存在一个代数求根公式，其中仅仅包含 F 的实根式.

证明 利用反证法. 设定理不真，即此三次方程的某一根可用 F 的实根式表出. 这就是说某一根 y_1 属于由 F 添加若干个实根式而生成的域 $L=F(\sqrt[r]{a}, \sqrt[s]{b}, \cdots)$. 因为 $D>0$，所以 $\sqrt{D}$ 亦是实根式. 故将 $\sqrt{D}$ 再添加到 L 上去而生成的扩域 $K=L(\sqrt{D})$ 亦是实域. 由本节的辅助定理 1 知道此三次方程的根均在 K 中，所以它们都可用仅含实根式的代数公式表出.

显然 $F\subset F(\sqrt{D})\subset K$，设方程 $y^3+py+q=0$ 的根域为 N，因为方程在域 F 中不可约，所以它的根不在 F 或 $F(\sqrt{D})$ 中，故 $F(\sqrt{D})\subset N\subset K$. 而 N 是由 $F(\sqrt{D})$ 添加有限个实根式所生成的：

$$F(\sqrt{D})\subset K_1\subset K_2\cdots\subset K_s=N,$$

这里 $K_{i+1}=K_i(a_i^{1/r_i})$，a_i 属于 K_i，r_i 是素数，$[K_{i+1}:K_i]=r_i$. 任取方程 $y^3+py+q=0$ 的一个根 y_1，则因 y_1 不在 $F(\sqrt{D})$ 中，而在 N 中，所以 y_1 必在某一个 K_{j+1} 中，而不在前一个 K_j 中. 于是 $r_j=3$，而扩域 $K_{j+1}=K_j(a_j^{1/r_j})$ 中所添加的是一个三次方根 $\sqrt[3]{a}$，因 K_{j+1} 是包含 $\sqrt{D}$ 的数域 K_j，添加方程 $y^3+py+q=0$ 的一个根 y_1 而生成，所以由辅助定理 1 知它包含此方程的所有根，因此 K_{j+1} 是这方程的根域，因而是正规域(见第 65 页). 由于 $\sqrt[3]{a}$ 属于 K_{j+1}，而 $\sqrt[3]{a}$ 是方程 $x^3-a=0$ 的一个根，所以 K_{j+1} 必须包含 $x^3-a=0$ 的所有根，即 $\sqrt[3]{a}$，$\omega\sqrt[3]{a}$，$\omega^2\sqrt[3]{a}$. 故 K_{j+1} 必包含 1 的三次虚根 ω. 这与 $K_{j+1}\subset K$ 是实域矛盾. 故定理得证.